QUATERNION GROUPS AND SUBGROUPS

MATH40000 Project

May 8, 2024

Joseph Brennan, id 10704601

School of Mathematics, University of Manchester

Contents

Abstract

This project focuses on the quaternions which is an algebra over the real numbers in four dimensions and denoted $\mathbb{H}$. We will learn about the properties of elements in $\mathbb{H}$ so that we can use them to prove many results throughout the project. We will also find out what types of groups can be represented by quaternions via homomorphism and what properties these groups have. Then once we have these groups and the homomorphisms between them, we aim to use their properties to show what the finite subgroups of the quaternions are.

Chapter 1

Introduction

We begin the project by defining the structure of the quaternions and describing their basic properties which will build the foundation that will help us to prove results throughout the project. To do this we will use quite a few standard definitions that can be found in many outside sources. It was not too difficult to prove a lot of the early results as they follow from the definition of the quaternion algebra, denoted as $\mathbb{H}$. However, a lot of these early results will be very important to us when it comes to proving more difficult results in the subsequent chapters. Proposition 2.3.5 about properties of $\mathbb{H}$ will be one of the most frequently used results when proving other propositions and lemmas later in the project. On the other hand, actually proving Proposition 2.3.5 is relatively easy since it is mostly just manipulation of the conjugate, norm, and trace of elements in $\mathbb{H}$.

After finding out about the properties of the quaternion algebra we will start to look at groups. The set of all quaternions except for 0, denoted $\mathbb{H}\backslash\{0\}$, forms a group and we will define subgroups of $\mathbb{H}\backslash\{0\}$. The most important of these subgroups will be the unit quaternions, denoted S^3 (quaternions with norm 1). We will define maps for elements in S^3 so that we can prove that there are homomorphisms from the unit quaternions to other groups that have interesting properties. These groups include the special orthogonal groups, $SO_4(\mathbb{R})$ and $SO_3(\mathbb{R})$, and the special unitary group, $SU_2(\mathbb{C})$. By isomorphism, we will prove that $SU_2(\mathbb{C})$ is also a subgroup of $\mathbb{H}\backslash\{0\}$. The results in this part of the project are trickier to prove than the initial properties. The results are more abstract, meaning that the proofs are more detailed.

However, a lot of the results will be very interesting and will show that there are a lot of powerful properties that come from the subgroups of quaternions. In particular, we will construct a homomorphism $B : S^3 \to SO_3(\mathbb{R})$ such that $B(q)$ represents a rotation in 3 dimensions, and this property will turn out to be very important later on.

In the final chapter we will define cyclic groups and the binary dihedral groups. Then we will use the fact that $B(q)$ can represent a rotation to calculate the trace of elements $q \in S^3$ depending on their order. We will use the results from the calculations to help us define the binary tetrahedral, octahedral, and icosahedral groups. We will also use results proved in earlier chapters to show that these five groups are all finite subgroups of the quaternions which will be the final result of the course. An even stronger result is that every subgroup of $\mathbb{H}\backslash\{0\}$ is conjugate (in S^3) to one of the five groups. However, proving this would require a lot more time which I unfortunately did not have. I found that the concepts from this chapter were the most challenging of the whole project which is why I may not have given proofs for every result in this chapter. However, I think it contains some of the most fascinating results of the project.

This project heavily focuses on algebra, groups, and subgroups, meaning that the results are quite abstract. We will see many propositions and lemmas which all have corresponding proofs. The majority of the proofs have been developed by myself, although some of them are expansions of proofs written by Lehrer and Taylor [1] where I have added more detail. There will be references for any results that are not proved in this project as well as for the diagrams and the more general definitions.

Chapter 2

The Basics of Quaternion Algebra

We will begin this project by learning about the basic definitions and properties of the quaternion algebra. What we will learn in this chapter will create a foundation that we will need to prove more significant results later in the project. Our aim in this chapter is to define the quaternion algebra along with the conjugate, norm, and trace of a quaternion. There will also be many other properties of the quaternions discussed in this chapter.

2.1 The Definition of Quaternion Algebra

In this first section, we will introduce and define the quaternions. To do so, the first thing we need is a general definition of an algebra which we can find in many sources such as "Associative Algebras" by Pierce [2].

Definition 2.1.1 (Algebra [2])**.** Let A be a vector space over a field F equipped with multiplication $* : A \times A \to A$. Then A is an *algebra* over F if $\forall x, y, z \in A$ and $\forall \lambda, \mu \in F$:

1. $(x + y) * z = x * z + y * z$,
2. $z * (x + y) = z * x + z * y$,
3. $(\lambda x) * (\mu y) = (\lambda\mu)(x * y)$.

We will now follow this up with the definitions of two types of algebra that have certain unique properties seen in "Abstract Algebra" by Dummit and Foote [3].

Definition 2.1.2 (Associative Algebra [3])**.** An algebra A over a field F is an *associative algebra* if $\forall x, y, z \in A$ we have

$$x * (y * z) = (x * y) * z.$$

Definition 2.1.3 (Unital Algebra [2])**.** An associative algebra A over a field F is also a *unital algebra* if and only if $\exists 1_A \in A$ such that $\forall x \in A$

$$x * 1_A = 1_A * x = x.$$

Another type of algebra is commutative algebra and we will define what it means for two elements to be commutative as follows.

Definition 2.1.4 (Commutative [3])**.** A binary operation $*$ on an algebra A is *commutative* if $\forall x, y \in A$

$$x * y = y * x.$$

If the property above is not satisfied then the binary operation is *non-commutative.*

An example of an algebra that we know of is the *complex numbers*, $\mathbb{C}$, over the field $\mathbb{R}$ (the real numbers). This algebra is associative, unital, and commutative. A basis for the complex numbers is $\{1, i\}$ which means that any $\alpha \in \mathbb{C}$ is uniquely written as $a1 + bi$ where $a, b \in \mathbb{R}$.

The set $M_2(\mathbb{R})$ of all 2×2 matrices with real-valued entries with multiplication as the binary operation is also an algebra over $\mathbb{R}$. It is an associative unital algebra like the complex numbers. However, by looking at an example we can show that $M_2(\mathbb{R})$ is non-commutative:

$$\begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix} \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}$$
$$\begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix} \neq \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix} \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix}.$$

Now we have introduced the general definition of an algebra and some of its types, we are ready to introduce the quaternions.

Definition 2.1.5 (Quaternions [1])**.** The *quaternions*, $\mathbb{H}$, is an algebra over $\mathbb{R}$ with basis $\{1, i, j, k\}$ where 1 is the identity element. $\mathbb{H}$ has multiplication as the binary operation defined by

$$\begin{aligned} jk &= i, & ki &= j, & ij &= k, \\ kj &= -i, & ik &= -j, & ji &= -k, \end{aligned}$$

and

$$i^2 = j^2 = k^2 = -1,$$

which is extended from the basis onto the whole space $\mathbb{H}$ by bilinearity.

Remark The binary operation is non-commutative because there exist some $q, r \in \mathbb{H}$ such that $qr \neq rq$. We write a quaternion in the form $a_0 + a_1 i + a_2 j + a_3 k$ where $a_0, a_1, a_2, a_3 \in \mathbb{R}$.

Example 2.1.6. $q = 2 + 3i + j$, $r = i - 2k$.

$$\begin{aligned} qr = (2 + 3i + j)(i - 2k) &= 2i - 4k + 3i^2 - 6ik + ji - 2jk \\ &= -3 + 6j - 5k, \end{aligned}$$

$$\begin{aligned} rq = (i - 2k)(2 + 3i + j) &= 2i + 3i^2 + ij - 4k - 6ki - 2kj \\ &= -3 + 4i - 6j - 3k \\ &\neq qr. \end{aligned}$$

The following lemma is a simple property of $\mathbb{H}$ that comes straight from the definition.

Lemma 2.1.7. *$ijk = -1$.*

Proof. We can see by using the definition of $\mathbb{H}$ that

$$ijk = i(jk) = i(i) = i^2 = -1.$$

□

Example 2.1.6 shows that quaternions do not always commute, thus showing how $\mathbb{H}$ is a non-commutative algebra. However, we see that real numbers commute with i, j and k. In fact, real numbers commute with all quaternions and we will prove that they are the only type of numbers to do so in the following proposition. Note here that the term *centre* means the set of elements that commute with every element in $\mathbb{H}$.

Proposition 2.1.8. *The centre of the quaternions is the real numbers ($Z(\mathbb{H}) = \mathbb{R}$).*

Proof. Suppose $q = a_0 + a_1 i + a_2 j + a_3 k \in Z(\mathbb{H})$, where $a_0, a_1, a_2, a_3 \in \mathbb{R}$. For q to be central in $\mathbb{H}$ it must commute with all elements in $\mathbb{H}$. We already know q will commute with any real number so we only need to check if q commutes with quaternion basis elements i, j, k.

Firstly we have

$$\begin{aligned} qi = (a_0 + a_1 i + a_2 j + a_3 k)i &= a_0 i + a_1 i^2 + a_2 ji + a_3 ki \\ &= a_0 i - a_1 - a_2 k + a_3 j \end{aligned}$$

and

$$\begin{aligned} iq = i(a_0 + a_1 i + a_2 j + a_3 k) &= a_0 i + a_1 i^2 + a_2 ij + a_3 ik \\ &= a_0 i - a_1 + a_2 k - a_3 j. \end{aligned}$$

Now since $q \in Z(\mathbb{H})$, assume that $qi = iq$. Then we have

$$\begin{aligned} qi = iq &\implies a_0 i - a_1 - a_2 k + a_3 j = a_0 i - a_1 + a_2 k - a_3 j \\ &\implies 2a_2 k - 2a_3 j = 0 \\ &\implies a_2 k = a_3 j. \end{aligned}$$

Since k and j are, by definition, linearly independent in $\mathbb{H}$, a_2 and a_3 must be equal to zero.

Next, we have

$$\begin{aligned} qj = (a_0 + a_1 i + a_2 j + a_3 k)j &= a_0 j + a_1 ij + a_2 j^2 + a_3 kj \\ &= a_0 j + a_1 k - a_2 - a_3 i \end{aligned}$$

and

$$\begin{aligned} jq = j(a_0 + a_1 i + a_2 j + a_3 k) &= a_0 j + a_1 ji + a_2 j^2 + a_3 jk \\ &= a_0 j - a_1 k - a_2 + a_3 i. \end{aligned}$$

Now since $q \in Z(\mathbb{H})$, assume that $qj = jq$. Then we have

$$\begin{aligned} qj = jq &\implies a_0 j + a_1 k - a_2 - a_3 i = a_0 j - a_1 k - a_2 + a_3 i \\ &\implies 2a_1 k - 2a_3 i = 0 \\ &\implies a_1 k = a_3 i. \end{aligned}$$

Since $k \neq 0$, then a_1 must also be equal to zero. We do not need to check $qk = kq$ since we already have $a_1 = a_2 = a_3 = 0$ and we know that $q = a_0$ commutes with k. Hence we are left with $q = a_0 + 0i + 0j + 0k \in Z(\mathbb{H})$ and so $q \in Z(\mathbb{H})$ if and only if q is real. Therefore $Z(\mathbb{H}) = \mathbb{R}$. □

We have shown that the quaternions are a non-commutative algebra and we have now proved that the centre of $\mathbb{H}$ is the real numbers. However, we also introduced the definitions an associative algebra and a unital algebra which we will now use to prove the following lemma.

Lemma 2.1.9. *$\mathbb{H}$ is an associative unital algebra.*

Proof. Given $q, r, s \in \mathbb{H}$, write $q = a_0 + a_1 i + a_2 j + a_3 k$, $r = b_0 + b_1 i + b_2 j + b_3 k$, $s = c_0 + c_1 i + c_2 j + c_3 k$ where the coefficients $a_0, \ldots, a_3, b_0, \ldots, b_3, c_0, \ldots, c_3$ are real numbers. First let us compute qr:

$$\begin{aligned} qr &= (a_0 + a_1 i + a_2 j + a_3 k)(b_0 + b_1 i + b_2 j + b_3 k) \\ &= (a_0 b_0 - a_1 b_1 - a_2 b_2 - a_3 b_3) + (a_0 b_1 + a_1 b_0 + a_2 b_3 - a_3 b_2) i \\ &+ (a_0 b_2 - a_1 b_3 + a_2 b_0 + a_3 b_1) j + (a_0 b_3 + a_1 b_2 - a_2 b_1 + a_3 b_0) k. \end{aligned}$$

Simplify the terms so we have $qr = \alpha + \beta i + \gamma j + \delta k$ such that

$$\begin{aligned} \alpha &= a_0 b_0 - a_1 b_1 - a_2 b_2 - a_3 b_3, \\ \beta &= a_0 b_1 + a_1 b_0 + a_2 b_3 - a_3 b_2, \\ \gamma &= a_0 b_2 - a_1 b_3 + a_2 b_0 + a_3 b_1, \\ \delta &= a_0 b_3 + a_1 b_2 - a_2 b_1 + a_3 b_0. \end{aligned}$$

Now we compute $(qr)s$ in terms of $\alpha, \beta, \gamma, \delta$.

$$\begin{aligned}(qr)s &= (\alpha + \beta i + \gamma j + \delta k)(c_0 + c_1 i + c_2 j + c_3 k)\\ &= \alpha(c_0 + c_1 i + c_2 j + c_3 k) + \beta(c_0 i - c_1 + c_2 k - c_3 j)\\ &+ \gamma(c_0 j - c_1 k - c_2 + c_3 i) + \delta(c_0 k + c_1 j - c_2 i - c_3).\end{aligned}$$

The q terms a_0, a_1, a_2, a_3 each appear exactly once in each term of the above result. Therefore we can rewrite the equation in terms of $a_0, a_1 i, a_2 j, a_3 k$:

$$\begin{aligned}(qr)s = a_0&[(b_0c_0 - b_1c_1 - b_2c_2 - b_3c_3) + (b_0c_1 + b_1c_0 + b_2c_3 - b_3c_2)i\\ &+ (b_0c_2 - b_1c_3 + b_2c_0 + b_3c_1)j + (b_0c_3 + b_1c_2 - b_2c_1 + b_3c_0)k]\\ &+ a_1 i[(b_0c_0 - b_1c_1 - b_2c_2 - b_3c_3) + (b_0c_1 + b_1c_0 + b_2c_3 - b_3c_2)i\\ &+ (b_0c_2 - b_1c_3 + b_2c_0 + b_3c_1)j + (b_0c_3 + b_1c_2 - b_2c_1 + b_3c_0)k]\\ &+ a_2 j[(b_0c_0 - b_1c_1 - b_2c_2 - b_3c_3) + (b_0c_1 + b_1c_0 + b_2c_3 - b_3c_2)i\\ &+ (b_0c_2 - b_1c_3 + b_2c_0 + b_3c_1)j + (b_0c_3 + b_1c_2 - b_2c_1 + b_3c_0)k]\\ &+ a_3 k[(b_0c_0 - b_1c_1 - b_2c_2 - b_3c_3) + (b_0c_1 + b_1c_0 + b_2c_3 - b_3c_2)i\\ &+ (b_0c_2 - b_1c_3 + b_2c_0 + b_3c_1)j + (b_0c_3 + b_1c_2 - b_2c_1 + b_3c_0)k]\\ &= (a_0 + a_1 i + a_2 j + a_3 k)[(b_0c_0 - b_1c_1 - b_2c_2 - b_3c_3) + (b_0c_1 + b_1c_0 + b_2c_3 - b_3c_2)i\\ &+ (b_0c_2 - b_1c_3 + b_2c_0 + b_3c_1)j + (b_0c_3 + b_1c_2 - b_2c_1 + b_3c_0)k]\\ &= q(rs),\end{aligned}$$

as required. Therefore by definition $\mathbb{H}$ is associative.

By definition of multiplication in $\mathbb{H}$, 1 is the identity element, so $\mathbb{H}$ is unital. □

Remark The algebra $\mathbb{H}$ has properties similar to $M_2(\mathbb{R})$ as they are both associative, unital, and non-commutative. Moreover, both have dimension 4 over $\mathbb{R}$.

2.2 The Conjugate, Norm, and Trace of a Quaternion

We will now define the conjugate, the norm, and the trace of a quaternion. These are three very important properties that will be used to prove many results later in the project.

Definition 2.2.1 (Conjugate of a quaternion [1])**.** Given $q \in \mathbb{H}$, written as $q = a_0 + a_1 i + a_2 j + a_3 k$ (where $a_0, ..., a_3 \in \mathbb{R}$), the *conjugate* of q is given by $\overline{q} = a_0 - a_1 i - a_2 j - a_3 k$.

Definition 2.2.2 (Norm of a quaternion [1])**.** The *norm* on $\mathbb{H}$ is the function $N : \mathbb{H} \to \mathbb{R}_{\geq 0}$ given by

$$N(q) = q\overline{q}$$

where $q \in \mathbb{H}$.

We can prove that the norm function on $\mathbb{H}$ has co-domain $\mathbb{R}_{\geq 0}$ by letting $q = a_0 + a_1 i + a_2 j + a_3 k$ (where $a_0, ..., a_3 \in \mathbb{R}$). Then we have

$$\begin{aligned} N(q) = q\bar{q} &= (a_0 + a_1 i + a_2 j + a_3 k)(a_0 - a_1 i - a_2 j - a_3 k) \\ &= a_0^2 - a_1^2 i^2 - a_2^2 j^2 - a_3^2 k^2 \\ &= a_0^2 + a_1^2 + a_2^2 + a_3^2 \in \mathbb{R}_{\geq 0}. \end{aligned}$$

We see here that $N(q)$ is clearly a non-negative real number as it is the sum of the squares of each coefficient of q. This also shows that $N(q) = 0$ if and only if $q = 0$.

Definition 2.2.3 (Trace of a quaternion [1])**.** The *trace* is a function $Tr : \mathbb{H} \to \mathbb{R}$ given by

$$Tr(q) = q + \bar{q}$$

where $q \in \mathbb{H}$.

In terms of the coefficients of q we have

$$\begin{aligned} Tr(a_0 + a_1 i + a_2 j + a_3 k) &= a_0 + a_1 i + a_2 j + a_3 k + a_0 - a_1 i - a_2 j - a_3 k \\ &= 2a_0. \end{aligned}$$

Just like with the norm, we see that the trace of a quaternion is also a real number. However, $Tr(q)$ can also be negative. This also shows that $Tr(q) = 0$ if and only if the real part of q is equal to 0.

Next we will define a division algebra and show that $\mathbb{H}$ is a division algebra by using the conjugate and the norm.

Definition 2.2.4 (Division Algebra [2])**.** A *division algebra* is an associative unital algebra A over a field F such that $\forall x \in A \backslash \{0_A\}$ there exists x^{-1} where $xx^{-1} = x^{-1}x = 1_A$.

Lemma 2.2.5. *Let $q \in \mathbb{H}$ with $q \neq 0$. Then an inverse q^{-1} exists.*

Proof. Write q in the form $q = a_0 + a_1 i + a_2 j + a_3 k$ with $q \neq 0$. Define $q^{-1} = N(q)^{-1}\overline{q}$. As we have seen previously, $N(q) = q\overline{q} = a_0^2 + a_1^2 + a_2^2 + a_3^2$ which is a positive real number (since $q \neq 0$). Positive real numbers have an inverse by definition so we can write $N(q)^{-1} = \frac{1}{q\overline{q}}$. Now we can check $qq^{-1} = q^{-1}q = 1$.

$$qq^{-1} = qN(q)^{-1}\overline{q} = \frac{q\overline{q}}{N(q)} = \frac{N(q)}{N(q)} = 1$$

$$q^{-1}q = N(q)^{-1}\overline{q}q = \frac{\overline{q}q}{N(q)} = \frac{N(\overline{q})}{N(q)}.$$

It remains to note that $N(q) = N(\overline{q}) = a_0^2 + a_1^2 + a_2^2 + a_3^2$ so $q^{-1}q = 1$. Hence q^{-1} exists. □

By the result of Lemma 2.2.5 we see from the definition that we have shown that the quaternions are a division algebra.

Definition 2.2.6 (Isomorphism [3])**.** An *isomorphism* from A to B (where A and B are associative unital algebras) is a bijective linear map $\rho : A \to B$ such that

(i) $\rho(1_A) = 1_B$,

(ii) for all $a_1, a_2 \in A$, $\rho(a_1 * a_2) = \rho(a_1) * \rho(a_2)$.

We say that a A is isomorphic to B (notated $A \cong B$) if there exists an isomorphism $\rho : A \to B$.

Remark Note that an algebra that is isomorphic to a division algebra must itself also be a division algebra. Lemma 2.2.5 shows us that $\mathbb{H}$ is a division algebra over $\mathbb{R}$. However, elements of $M_2(\mathbb{R})$ that have a zero determinant do not have an inverse. Therefore despite being similar, $\mathbb{H}$ and $M_2(\mathbb{R})$ are not isomorphic since $M_2(\mathbb{R})$ is not a division algebra.

2.3 More Properties of the Quaternions

We can now use what we have seen from the previous two sections to prove some less obvious properties of the quaternions.

Definition 2.3.1 (Subalgebra [3])**.** Given an associative unital algebra A, a *subalgebra* is a subspace of A that is closed under multiplication of A and contains 1_A. Note that a subalgebra is also an associative unital algebra with induced operations.

By Lemma 2.1.9, the quaternions are an associative unital algebra. We have also seen that the complex numbers are associative and unital. By using the definition of a subalgebra and what it means for two algebras to be isomorphic, we can prove the following lemma.

Lemma 2.3.2. *The complex numbers* $\mathbb{C}$ *viewed as an algebra over* $\mathbb{R}$ *is isomorphic to the subalgebra of* $\mathbb{H}$ *spanned by 1 and* i*.*

Proof. Define a function $\rho : \mathbb{C} \to span_{\mathbb{H}}\{1, i\}$ such that for $\alpha + \beta i \in \mathbb{C}$ we have $\rho(\alpha + \beta i) = \alpha + \beta i + 0j + 0k$. Firstly, to show that ρ is a homomorphism we need to show that:

1. $\forall z_1, z_2 \in \mathbb{C}$, $\rho(z_1 + z_2) = \rho(z_1) + \rho(z_2)$,
2. $\forall z \in \mathbb{C}$ and $r \in \mathbb{R}$, $\rho(rz) = r\rho(z)$,
3. $\forall z_1, z_2 \in \mathbb{C}$, $\rho(z_1 z_2) = \rho(z_1)\rho(z_2)$,
4. $\rho(1_{\mathbb{C}}) = 1_{\mathbb{H}}$.

(1) and (2) tell us that ρ is a linear map and (3) shows that ρ is multiplicative.
To show (1) let $z_1 = \alpha_1 + \beta_1 i$ and $z_2 = \alpha_2 + \beta_2 i$. Then

$$\begin{aligned}
\rho(z_1 + z_2) &= \rho((\alpha_1 + \beta_1 i) + (\alpha_2 + \beta_2 i)) \\
&= \rho((\alpha_1 + \alpha_2) + (\beta_1 + \beta_2)i) \\
&= (\alpha_1 + \alpha_2) + (\beta_1 + \beta_2)i + 0j + 0k \\
&= (\alpha_1 + \beta_1 i + 0j + 0k) + (\alpha_2 + \beta_2 i + 0j + 0k) \\
&= \rho(z_1) + \rho(z_2).
\end{aligned}$$

To show (2) let $z = \alpha + \beta i$. Then

$$\begin{aligned}\rho(rz) &= \rho(r(\alpha + \beta i)) \\ &= \rho(r\alpha + r\beta i) \\ &= r\alpha + r\beta i + 0j + 0k \\ &= r(\alpha + \beta i + 0j + 0k) \\ &= r\rho(z).\end{aligned}$$

To show (3) let $z_1 = \alpha_1 + \beta_1 i$ and $z_2 = \alpha_2 + \beta_2 i$. Then

$$\begin{aligned}\rho(z_1 z_2) &= \rho((\alpha_1 + \beta_1 i)(\alpha_2 + \beta_2 i)) \\ &= \rho((\alpha_1\alpha_2 - \beta_1\beta_2) + (\alpha_1\beta_2 + \alpha_2\beta_1)i) \\ &= (\alpha_1\alpha_2 - \beta_1\beta_2) + (\alpha_1\beta_2 + \alpha_2\beta_1)i + 0j + 0k \\ &= (\alpha_1 + \beta_1 i + 0j + 0k)(\alpha_2 + \beta_2 i + 0j + 0k) \\ &= \rho(z_1)\rho(z_2).\end{aligned}$$

To show (4) we have that $1_{\mathbb{C}} = 1 + 0i$. Then

$$\rho(1 + 0i) = 1 + 0i + 0j + 0k = 1_{\mathbb{H}}.$$

Hence we have shown that ρ is a homomorphism. We now need to check that ρ is a bijection for it to be an isomorphism.

Assume $\rho(z_1) = \rho(z_2)$ for some $z_1, z_2 \in \mathbb{C}$. Then $\rho(\alpha_1 + \beta_1 i) = \rho(\alpha_2 + \beta_2 i) \Rightarrow \alpha_1 + \beta_1 i + 0j + 0k = \alpha_2 + \beta_2 i + 0j + 0k$. By comparing the coefficients of $1, i, j, k$, we see that $\alpha_1 = \alpha_2$ and $\beta_1 = \beta_2$. Therefore ρ is injective.

All quaternions $q \in span_{\mathbb{H}}\{1, i\}$ are of the form $q = \alpha + \beta i + 0j + 0k$ where $\alpha, \beta \in \mathbb{R}$. Clearly there exists $z \in \mathbb{C}$ such that $\rho(z) = q$. Then $z = \alpha + \beta i \Rightarrow \rho(z) = \alpha + \beta i + 0j + 0k \in span_{\mathbb{H}}\{1, i\}$. Hence ρ is surjective and therefore also bijective.

Therefore $\mathbb{C} \cong span_{\mathbb{H}}\{1, i\}$. □

By isomorphism, Lemma 2.3.2 shows that $\mathbb{C}$ itself is a subalgebra of $\mathbb{H}$. We can now expand on the relationship between the quaternions and the complex numbers by proving the next two corollaries.

Corollary 2.3.3. *For all $q \in \mathbb{H}$, there exists unique $\alpha, \beta \in \mathbb{C}$ such that $q = \alpha + \beta j$.*

Proof. Let $q = a_0 + a_1 i + a_2 j + a_3 k$. We want to express q in the form $\alpha + \beta j$ where $\alpha, \beta \in \mathbb{C}$. The first two terms of q, $a_0 + a_1 i$ are a complex number so denote them as $\alpha = a_0 + a_1 i$ so that we have $q = \alpha + a_2 j + a_3 k$. Then we can rewrite the terms $a_2 j + a_3 k$ as

$$a_2 j + a_3 k = (a_2 - a_3 kj)j = (a_2 + a_3 i)j$$

since $i = -kj$ by definition. We can now denote $\beta = a_2 + a_3 i$ as it is a complex number. We now have $q = \alpha + \beta j$ as required so we have proved existence.

Now to show uniqueness, assume that there exists two complex numbers such that for $\beta = x + yi$ we have

$$q = (a_0 + a_1 i) + (x + yi)j = (b_0 + b_1 i) + (x + yi)j$$

By comparing terms we see that for the equation to be true we must have that $a_0 + a_1 i = b_0 + b_1 i$ and $x + yi = x + yi$. For this to be the case then $a_0 = b_0$ and $a_1 = b_1$. Therefore α and β are unique. □

Corollary 2.3.4. $\mathbb{H}$ *is a vector space over* $\mathbb{C}$.

Proof. For $\mathbb{H}$ to be a vector space over $\mathbb{C}$ it needs to satisfy ten axioms. Many of these axioms are already satisfied by the definition of $\mathbb{H}$ and the fact that $\mathbb{H}$ is an associative unital algebra so we only need to show a few.

We can see that $\mathbb{H}$ is closed under left multiplication by elements of $\mathbb{C}$ since $\mathbb{C} = span_{\mathbb{H}}\{1, i\}$. So if z is a complex number, then it is also a quaternion with zero coefficients for j and k. Hence $z \in \mathbb{C}, q \in \mathbb{H} \implies zq \in \mathbb{H}$.

Next, we need to show that $\mathbb{H}$ satisfies distributivity over $\mathbb{C}$:

1. $(z_1 + z_2)q = z_1 q + z_2 q$ for $z_1, z_2 \in \mathbb{C}$ for any $z_1, z_2 \in \mathbb{C}$ and $q \in \mathbb{H}$,
2. $z(q + r) = zq + zr$ for $z \in \mathbb{C}$ and $q, r \in \mathbb{H}$,
3. $(z_1 z_2)q = z_1(z_2 q)$ for any $z_1, z_2 \in \mathbb{C}$ and $q \in \mathbb{H}$,
4. $1_{\mathbb{C}} q = q$ for all $q \in \mathbb{H}$.

We know that (1)-(3) are satisfied by the axioms of an algebra. Then (4) is true because $1_{\mathbb{C}} = 1_{\mathbb{H}}$ and by the definition of $1_{\mathbb{H}}$ as the identity element of $\mathbb{H}$. Since $\mathbb{H}$ satisfies all the required axioms we have now shown that it is a vector space over $\mathbb{C}$. □

Remark Although the quaternions are a vector space over the complex numbers, it is not an algebra over them. We see this since the third axiom of the algebra definition would not be satisfied.

Now we will prove several more properties of the quaternions in the following proposition.

Proposition 2.3.5 (Properties of $\mathbb{H}$). *(i) If $q = \alpha + \beta j$ with $\alpha, \beta \in \mathbb{C}$, then $\overline{q} = \overline{\alpha} - \beta j$, $N(q) = \alpha\overline{\alpha} + \beta\overline{\beta}$ and $Tr(q) = \alpha + \overline{\alpha}$.*

(ii) $\overline{q + r} = \overline{q} + \overline{r}$, $\overline{qr} = \overline{r}\,\overline{q}$, *and* $\overline{\overline{q}} = q$.

(iii) $N(qr) = N(q)N(r)$.

(iv) $Tr(q + r) = Tr(q) + Tr(r)$.

(v) $Tr(qr) = Tr(rq)$.

(vi) $q^2 - Tr(q)q + N(q) = 0$.

(vii) $Tr(q\overline{r}) = N(q + r) - N(q) - N(r)$.

Proof. (i) Let $q = a_0 + a_1 i + a_2 j + a_3 k$ where $a_0, a_1, a_2, a_3 \in \mathbb{R}$. Then we can rearrange to get $q = (a_0 + a_1 i) + (a_2 + a_3 i)j = \alpha + \beta j$ since $ij = k$. Then if we have $\overline{q} = a_0 - a_1 i - a_2 j - a_3 k$, we can similarly rearrange to get $\overline{q} = (a_0 - a_1 i) - (a_2 + a_3 i)j = \overline{\alpha} - \beta j$.

Now we have shown what q and $\overline{q}$ are in terms of α and β we can show what the norm and trace are. Firstly we get the following for the norm:

$$\begin{aligned}
N(q) &= q\overline{q} && \text{(by Definition 2.4)}\\
&= (\alpha + \beta j)(\overline{\alpha} - \beta j)\\
&= \alpha\overline{\alpha} - \alpha\beta j + \beta j\overline{\alpha} + \beta j(-\beta j)\\
&= \alpha\overline{\alpha} - \alpha\beta j + \alpha\beta j - \beta j(j\overline{\beta}) && (\text{since } \overline{\alpha}j = j\alpha)\\
&= \alpha\overline{\alpha} + \beta\overline{\beta} && (\text{since } j^2 = -1).
\end{aligned}$$

Then we also get the following trace:

$$Tr(q) = q + \overline{q} = \alpha + \beta j + \overline{\alpha} - \beta j = \alpha + \overline{\alpha}.$$

(ii) Let $r = b_0 + b_1 i + b_2 j + b_3 k$ where $b_0, b_1, b_2, b_3 \in \mathbb{R}$. Then $q + r = a_0 + b_0 + (a_1 + b_1)i + (a_2 + b_2)j + (a_3 + b_3)k$ and we get

$$\begin{aligned}\overline{q+r} &= a_0 + b_0 - (a_1 + b_1)i - (a_2 + b_2)j - (a_3 + b_3)k \\ &= (a_0 - a_1 i - a_2 j - a_3 k) + (b_0 - b_1 i - b_2 j - b_3 k) \\ &= \overline{q} + \overline{r}.\end{aligned}$$

Next,

$$\begin{aligned}qr &= (a_0 + a_1 i + a_2 j + a_3 k)(b_0 + b_1 i + b_2 j + b_3 k) \\ &= (a_0 b_0 + a_1 b_1 + a_2 b_2 + a_3 b_3) + (a_0 b_1 + a_1 b_0 + a_2 b_3 - a_3 b_2)i \\ &+ (a_0 b_2 - a_1 b_3 + a_2 b_0 + a_3 b_1)j + (a_0 b_3 + a_1 b_2 - a_2 b_1 + a_3 b_0)k.\end{aligned}$$

From this, we get the conjugate,

$$\begin{aligned}\overline{qr} &= (a_0 b_0 + a_1 b_1 + a_2 b_2 + a_3 b_3) - (a_0 b_1 + a_1 b_0 + a_2 b_3 - a_3 b_2)i \\ &- (a_0 b_2 - a_1 b_3 + a_2 b_0 + a_3 b_1)j - (a_0 b_3 + a_1 b_2 - a_2 b_1 + a_3 b_0)k.\end{aligned}$$

Then rearrange $\overline{r}\overline{q}$ as follows:

$$\begin{aligned}\overline{r}\overline{q} &= (b_0 - b_1 i - b_2 j - b_3 k)(a_0 - a_1 i - a_2 j - a_3 k) \\ &= b_0 a_0 - b_1 a_1 - b_2 a_2 - b_3 a_3 - (b_0 a_1 + b_1 a_0 - b_2 a_3 + b_3 a_2)i \\ &- (b_0 a_2 + b_1 a_3 + b_2 a_0 - b_3 a_1)j - (b_0 a_3 - b_1 a_2 + b_2 c_1 + b_3 a_0)k \\ &= \overline{qr}.\end{aligned}$$

Since the coefficients a_n, b_n are real numbers they commute, so the above expressions for $\overline{qr}$ and $\overline{r}\overline{q}$ are equal.
Finally, if we have $\overline{q} = a_0 - a_1 i - a_2 j - a_3 k$, then we get

$$\begin{aligned}\overline{\overline{q}} &= a_0 - (-a_1 i) - (-a_2 j) - (-a_3 k) \\ &= a_0 + a_1 i + a_2 j + a_3 k = q.\end{aligned}$$

(iii) We have $N(qr) = qr\overline{qr} = qr\overline{r}\overline{q}$ (by (ii)). Then

$$\begin{aligned}qr\overline{r}\overline{q} &= qN(r)\overline{q} = q\overline{q}N(r) \qquad \text{(Since } N(r) \in \mathbb{R} \text{ and } Z(\mathbb{H}) = \mathbb{R}) \\ &= N(q)N(r).\end{aligned}$$

Thus we have shown that $N(qr) = N(q)N(r)$.

(iv) We have $Tr(q+r) = q+r+\overline{q+r} = q+r+\overline{q}+\overline{r}$ (by (ii)). Then we can rearrange to get $q+\overline{q}+r+\overline{r} = Tr(q)+Tr(r)$.

(v) Let q and r be represented by the coefficients in proof (ii). The real part of qr is $a_0b_0 - a_1b_1 - a_2b_2 - a_3b_3$. So $Tr(qr) = 2(a_0b_0 - a_1b_1 - a_2b_2 - a_3b_3)$ by the definition of trace.

Then similarly we get the real part of rq as $b_0a_0 - b_1a_1 - b_2a_2 - b_3a_3$. So $Tr(rq) = 2(b_0a_0 - b_1a_1 - b_2a_2 - a_3b_3)$. Thus, by the commutativity of the real numbers, $Tr(qr) = Tr(rq)$.

(vi) By using the definitions that $Tr(q) = q+\overline{q}$ and $N(q) = q\overline{q}$ we see that

$$\begin{aligned} q^2 - Tr(q)q + N(q) &= qq - (q+\overline{q})q + q\overline{q} \\ &= qq - qq - \overline{q}q + q\overline{q} \\ &= q\overline{q} - \overline{q}q = 0 \qquad\qquad \text{(since } q\overline{q} = \overline{q}q\text{)}. \end{aligned}$$

We know that $q\overline{q} = N(q) = N(\overline{q}) = \overline{q}q$ from the proof of Lemma 2.2.5.

(vii) We have $Tr(q\overline{r}) = q\overline{r} + \overline{q\overline{r}} = q\overline{r} + \overline{\overline{r}}\,\overline{q} = q\overline{r} + r\overline{q}$ since $\overline{\overline{r}} = r$. Then we get

$$\begin{aligned} N(q+r) - N(q) - N(r) &= (q+r)\overline{(q+r)} - q\overline{q} - r\overline{r} \\ &= (q+r)(\overline{q}+\overline{r}) - q\overline{q} - r\overline{r} \\ &= q\overline{q} + q\overline{r} + r\overline{q} + r\overline{r} - q\overline{q} - r\overline{r} \\ &= q\overline{r} + r\overline{q} = Tr(q\overline{r}). \end{aligned}$$

□

To prove the next corollary we will need to use the Rank-nullity theorem given by the following.

Theorem 2.3.6 (The Rank-Nullity Theorem [4])**.** *Let $T : V \to W$ be a linear map. Then* $\operatorname{rank} T + \operatorname{null} T = \dim V$ *where* $\operatorname{rank} T$ *is the dimension of the image W and where* $\operatorname{null} T$ *is the nullity of T (the dimension of its kernel).*
It follows that for linear transformations of vector spaces of equal finite dimension, either injectivity or surjectivity implies bijectivity.

We will not prove this theorem since we only need it to prove the next result. The Rank-Nullity Theorem is very well-known and we can see an explicit proof by Towers [4].

Corollary 2.3.7. *If $q \in \mathbb{H}$ and $q \notin \mathbb{R}$, then the field $\mathbb{R}[q]$ is isomorphic to the complex numbers $\mathbb{C}$.*

Proof. Part (vi) of the previous proposition tells us that every quaternion satisfies a quadratic equation with real coefficients. Therefore, every q^n can be written as $a + bq$ where $a, b \in \mathbb{R}$, and more generally, all elements of $\mathbb{R}[q]$ can be written in this form. Hence the field $\mathbb{R}[q]$ is a quadratic extension of the real numbers and can be written as $\mathbb{R}[q] = \{a + bq \mid a, b \in \mathbb{R}\}$. $\mathbb{R}[q]$ is a field because the inverse $(a + bq)^{-1} = \frac{a+b\overline{q}}{N(a+bq)}$ is still in $\mathbb{R}[q]$. The conjugate of q is $-q + x$ where x is a real number, so $\overline{q}$ also lies in $\mathbb{R}[q]$.

To check that $\mathbb{R}[q]$ is isomorphic to the complex numbers, $\mathbb{C} = \{a + bi \mid a, b \in \mathbb{R}\}$, we first need to see if there is a homomorphism. For two elements $a + bq$ and $c + dq$ in $\mathbb{R}[q]$ where $a, b, c, d \in \mathbb{R}$, we need define a map $\phi : \mathbb{R}[q] \to \mathbb{C}$ by $\phi(a + bq) = a + b\mu$ where μ satisfies the quadratic equation $\mu^2 - Tr(q)\mu + N(q) = 0$ from part (vi) of the previous proposition. We have that

$$\mu = \frac{Tr(q) \pm \sqrt{Tr(q)^2 - 4N(q)}}{2}$$

and if we let $q = a + bi + cj + dk$ where $b, c, d \in \mathbb{R}$ not all equal to 0, then the discriminant of μ is

$$Tr(q)^2 - 4N(q) = (2a)^2 - 4(a^2 + b^2 + c^2 + d^2) = -4(b^2 + c^2 + d^2).$$

The discriminant must be negative because it is the negation of the sum of real square numbers. Therefore μ is a complex number meaning that the image of ϕ is in $\mathbb{C}$.

Now we need to check that $\phi((a + bq) + (c + dq)) = \phi(a + bq) + \phi(c + dq)$ and $\phi((a + bq)(c + dq)) = \phi(a + bq)(c + dq)$. Firstly we have

$$\begin{aligned}
\phi((a + bq) + (c + dq)) &= \phi((a + c) + (b + d)q) \\
&= a + c + (b + d)\mu \\
&= (a + b\mu) + (c + d\mu) \\
&= \phi(a + bq) + \phi(c + dq).
\end{aligned}$$

Then

$$\begin{aligned}
\phi((a+bq)(c+dq)) &= \phi(ac+adq+bcq+bdq^2) \\
&= \phi[ac+(ad+bc)q+bd(Tr(q)q)-N(q))] && \text{(By Proposition 2.3.5(vi))} \\
&= \phi[(ac-N(q)bd)+(ad+bc+Tr(q)bd)q] \\
&= ac-N(q)bd+(ad+bc+Tr(q)bd)\mu \\
&= ac+ad\mu+bc\mu+bd(Tr(q)\mu-N(q)) \\
&= ac+ad\mu+bc\mu+bd\mu^2 && \text{(By Proposition 2.3.5(vi))} \\
&= (a+b\mu)(c+d\mu) \\
&= \phi(a+bq)\phi(c+dq).
\end{aligned}$$

Now we need to show that $\phi : \mathbb{R}[q] \to \mathbb{C}$ is a bijective map. Note that ϕ is a linear map of $\mathbb{R}$-vector spaces and that the $\dim_{\mathbb{R}} \mathbb{R}[q] = \dim_{\mathbb{R}} \mathbb{C} = 2$. By the Rank-nullity theorem, we have that $\operatorname{null}\phi = \dim_{\mathbb{R}} \mathbb{R}[q] - \dim_{\mathbb{R}} \mathbb{C} = 0$. So the nullity of ϕ is 0 meaning that $\ker\phi = 0$ which shows that ϕ is injective.

So it is enough to show that ϕ is surjective. We know that there exists $e, f \in \mathbb{R}$ such that $\phi(e+fq) = i$ since ϕ is a map from $\mathbb{R}[q]$ to $\mathbb{C}$ and $i \in \mathbb{C}$. We also know that $\phi(1+0q) = 1$. Therefore we have $\phi(a1+b(e+fq)) = a+bi$ for all $a, b \in \mathbb{R}$ and so ϕ is surjective.

Hence $\mathbb{R}[q]$ is isomorphic to $\mathbb{C}$. $\square$

A result we will not prove is that up to isomorphism, $\mathbb{H}$ is the only non-commutative division algebra over $\mathbb{R}$ with the property that each of its elements satisfies a polynomial equation with real coefficients (from Lehrer and Taylor [1]).

Chapter 3

Quaternion Groups

Now that we know about the quaternion algebra, we can use what we have learned about its properties to define subgroups of the group of non-zero quaternions, $\mathbb{H}\backslash\{0\}$. We will also prove useful results including homomorphisms from one of the subgroups of $\mathbb{H}\backslash\{0\}$ to other groups. The groups we will define in this chapter have interesting properties and the results from the previous chapter will help us prove that these properties are true.

3.1 Linear Transformations and Unit Quaternions

In the first section of this chapter we will learn about the most important subgroup of $\mathbb{H}\backslash\{0\}$, namely the group of unit quaternions, S^3. We will also define the group of linear transformations, $SL_4(\mathbb{R})$. After we have done this, we will aim to prove that there is a homomorphism from S^3 to $SL_4(\mathbb{R})$.

Before we define the group of linear transformations of $\mathbb{H}$, we will need some preliminary definitions. The first thing we need is to define a particular left multiplication and right multiplication of an element $q \in \mathbb{H}$ that we will use for the rest of this project. This definition is as follows.

Definition 3.1.1 (Transformations $L(q)$ and $R(q)$)**.** Multiplication by $q \in \mathbb{H}$ on the left defines the $\mathbb{R}$-linear transformation

$$\begin{aligned} L(q)\colon \mathbb{H} &\to \mathbb{H} \\ h &\mapsto qh. \end{aligned}$$

Multiplication by $\overline{q}$ on the right defines the $\mathbb{R}$-linear transformation

$$\begin{aligned} R(q)\colon \mathbb{H} &\to \mathbb{H} \\ h &\mapsto h\overline{q}. \end{aligned}$$

These two functions will be very important in this chapter since they are linear transformations. The notation $L(q)$ and $R(q)$ can be unclear as it may look like we are evaluating the variable q. However, we are actually evaluating another variable $h \in \mathbb{H}$ and defining left and right multiplication on h. Explicitly, we can rewrite this definition as

$$\begin{aligned} L(q)(h) &= qh \\ R(q)(h) &= h\overline{q}. \end{aligned}$$

Next we will discuss some properties of $L(q)$ and $R(q)$. Some of these properties involve the reflection of quaternions. Hence we will first define reflection which is a standard definition in geometry and can be found in books such as "Geometry Revisited" by Coxeter and Greitzer [5].

Definition 3.1.2 (Reflection in $\mathbb{R}^n$ [5])**.** In a Euclidean space $\mathbb{R}^n$, a *reflection* of a vector $q \in \mathbb{R}^n$ in the hyperplane orthogonal to $r \in \mathbb{R}^n$ through the origin is given by

$$Ref_r(q) = q - 2\frac{q \cdot r}{r \cdot r} r,$$

where $q \cdot r$ denotes the dot product of q with r.

Note that we can regard $\mathbb{H}$ as the 4-dimensional space $\mathbb{R}^4$. So for the reflection of a quaternion, we can use this definition for $\mathbb{R}^4$. In this case, we need to define the dot product between the two elements q and r when they are 4-dimensional. We need to define the dot product on $\mathbb{H}$.

Definition 3.1.3 (Dot product in $\mathbb{H}$)**.** The *dot product* of two elements $q, r \in \mathbb{H}$ is given by

$$q \cdot r = \begin{pmatrix} a_1 \\ b_1 \\ c_1 \\ d_1 \end{pmatrix} \cdot \begin{pmatrix} a_2 \\ b_2 \\ c_2 \\ d_2 \end{pmatrix} = a_1a_2 + b_1b_2 + c_1c_2 + d_1d_2,$$

where $q = a_1 + b_1i + c_1j + d_1k$ and $r = a_2 + b_2i + c_2j + d_2k$.

Now we can prove the following lemma which tells us an important property about reflection in $\mathbb{H}$ and links reflection with the linear transformations $L(q)$ and $R(q)$.

Lemma 3.1.4. *The map $\rho\colon \mathbb{H} \to \mathbb{H}$ given by $\rho(q) = -\overline{q}$ is a reflection with $\rho^2 = 1$ and $\rho L(q)\rho = R(q)$ for all $q \in \mathbb{H}$.*

Proof. The coordinates given by $\rho(q) = q$ give the 3-dimensional hyperplane that ρ is the reflection in. If $q = a + bi + cj + dk$ then $\rho(q) = -a + bi + cj + dk$ so ρ is a reflection in the hyperplane given by the vector $r = (1, 0, 0, 0) = 1_{\mathbb{H}}$. Then we have $q \cdot r = a$ and $r \cdot r = 1$ using the definition of the dot product. Then from the previous definition of a reflection we get

$$\begin{aligned} Ref_r(q) = q - 2\frac{q \cdot r}{r \cdot r}r &= (a, b, c, d) - 2\frac{a}{1}(1, 0, 0, 0) \\ &= (a, b, c, d) - (2a, 0, 0, 0) \\ &= (-a, b, c, d) = -a + bi + cj + dk = -\overline{q}. \end{aligned}$$

Hence we have the map $\rho(q) = -\overline{q}$. We can see that $\rho^2 = 1$ since $\rho(\rho(q)) = \rho(-\overline{q}) = \overline{\overline{q}} = q$. In fact, it is clear that any reflection squared gives the identity. We also see that

$$\rho L(q)\rho(h) = \rho L(q)(-\overline{h}) = \rho(-q\overline{h}) = h\overline{q} = R(q)(h),$$

as required. □

Remark Note that $\rho L(q)\rho(h)$ is equivalent to $(\rho \circ L(q) \circ \rho)(h)$, the composition of the functions.

We will prove another property of the linear transformations $L(q)$ and $R(q)$ which will link them to the norm of a quaternion. However, to prove that property we will need the result of this lemma which gives us an alternative way of viewing the quaternions.

Lemma 3.1.5. *We can regard $\mathbb{H}$ as a 2-dimensional vector space over the field $\mathbb{R}[q]$ with basis $\{1, r\}$ where $r \in \mathbb{H} \backslash \mathbb{R}[q]$.*

Proof. To show that $\{1, r\}$ is a basis for $\mathbb{H}$ over $\mathbb{R}[q]$ we must show 1 and r are linearly independent over $\mathbb{R}[q]$ and span the entire vector space.

1. *Linear independence:* Suppose that there exist $a + bq, c + dq \in \mathbb{R}[q]$ such that $(a+bq)(1)+(c+dq)(r) = 0$. Suppose $c+dq \neq 0$. Then $r = (c+dq)^{-1}(a+bq)(1)$. But here we have a contradiction since the right-hand side of the equation is in $\mathbb{R}[q]$ whereas r is not in $\mathbb{R}[q]$. Now suppose $c + dq = 0$. Then $a + bq = 0$ and so $a = -bq$. But here we have another contradiction since $-bq \in \mathbb{H} \backslash \mathbb{R}$ whereas $a \in \mathbb{R}$ by the definition of $\mathbb{R}[q]$. Therefore no linear combination of elements in $\mathbb{R}[q]$ exists with respect to the basis $\{1, r\}$ so 1 and r are linearly independent.

2. *Spanning the vector space:* The basis elements 1 and r span $1, q, r, qr$ over $\mathbb{R}[q]$. We claim that $1, q, r, qr$ are linearly independent over $\mathbb{R}$. Indeed, if $a1+bq+cr+dqr = 0$ with $a, b, c, d \in \mathbb{R}$ and not all equal to 0, then $(a+bq)(1)+(c+dq)(r) = 0$ which contradicts the linear independence of 1 and r over $\mathbb{R}[q]$. Since $\dim_{\mathbb{R}} \mathbb{H} = 4$, $\mathbb{H}$ is spanned by $1, q, r, qr$ over the real numbers. Therefore $\mathbb{H}$ is spanned by $1, r$ over $\mathbb{R}[q]$.

Hence we can regard $\mathbb{H}$ as a 2-dimensional vector space over $\mathbb{R}[q]$ with basis $\{1, r\}$. $\square$

The next proposition is going to be useful later in the section as it links linear transformations in $\mathbb{H}$ to the norm of a quaternion and we are aiming to prove that there is a homomorphism between groups with these kinds of properties. We will use the lemma above to prove this proposition which is as follows.

Proposition 3.1.6. *For any element $q \in \mathbb{H}$, $\det L(q) = \det R(q) = N(q)^2$.*

Proof. View $\mathbb{H}$ as a 4-dimensional vector space over $\mathbb{R}$. If $q \in \mathbb{R}$, then $N(q) = q\overline{q} = q^2$ since the conjugate of a real number is itself. We also have that

$$\begin{aligned} L(q)(h) &= qh = hq && \text{(since real numbers commute with all elements in } \mathbb{H}) \\ &= h\overline{q} = R(q)(h) \end{aligned}$$

and this is a scalar transformation with determinant $q^4 = N(q)^2$. Suppose that $q \notin \mathbb{R}$. We can regard $\mathbb{H}$ as a vector space over $\mathbb{R}[q]$ with basis $1, r$ by Lemma 3.1.5. Then $1, q, r, qr$ is a basis for $\mathbb{H}$ as a real space. Then the matrix of $L(q)$ with respect to this basis is computed by applying the map $L(q)$ explicitly to the basis vectors $1, q, r, qr$ as follows:

$$\begin{aligned} L(q)(1) &= q1 = 0(1) + 1(q) + 0(r) + 0(qr) \\ L(q)(q) &= qq = q^2 = Tr(q)q - N(q) && \text{(by Proposition 2.3.5(vi))} \\ &= -N(q)(1) + Tr(q)(q) + 0(r) + 0(qr) \\ L(q)(r) &= qr = 0(1) + 0(q) + 0(r) + 1(qr) \\ L(q)(qr) &= qqr = q^2r = Tr(q)qr - N(q)r && \text{(by Proposition 2.3.5(vi))} \\ &= 0(1) + 0(q) - N(q)(r) + Tr(q)(qr). \end{aligned}$$

Then by letting each computation of $L(q)$ above be represented by columns of a matrix with rows representing the coefficients we get

$$L(q) = \begin{pmatrix} 0 & -N(q) & 0 & 0 \\ 1 & Tr(q) & 0 & 0 \\ 0 & 0 & 0 & -N(q) \\ 0 & 0 & 1 & Tr(q) \end{pmatrix}.$$

Then from this matrix, we can compute the determinant

$$\det L(q) = N(q) \begin{vmatrix} 1 & 0 & 0 \\ 0 & 0 & -N(q) \\ 0 & 1 & Tr(q) \end{vmatrix} = N(q)(1 \times (N(q))) = N(q)^2.$$

Finally, we have

$$\begin{aligned}
\det(R(q)) &= \det(\rho L(q)\rho) && \text{(by Lemma 3.1.4)}\\
&= \det(\rho)\det(L(q))\det(\rho)\\
&= \det(\rho)\det(\rho)\det(L(q))\\
&= \det(\rho^2)\det(L(q))\\
&= \det(1)\det(L(q)) && \text{(by Lemma 3.1.4)}\\
&= \det(L(q)).
\end{aligned}$$

Hence $\det(L(q)) = \det(R(q)) = N(q)^2$. □

We now move on to one of the most important definitions which we will need throughout the rest of the project.

Definition 3.1.7 (Group of unit quaternions [1])**.** The set $S^3 := \{q \in \mathbb{H} \mid N(q) = 1\}$ is called the *group of unit quaternions*. S^3 can also be interpreted as the unit 3-sphere in $\mathbb{R}^4$.

Remark If we let $q = a_0 + a_1 i + a_2 j + a_3 k$, we have previously shown that $N(q) = a_0^2 + a_1^2 + a_2^2 + a_3^2$ and we can see that the equation $a_0^2 + a_1^2 + a_2^2 + a_3^2 = 1$ corresponds to the sphere of radius 1 in 4 dimensions. Hence every element of S^3 corresponds to the coordinates of a point of the unit 3-sphere.

It will now follow that the unit quaternions are a subgroup of $\mathbb{H}\backslash\{0\}$ which we prove as follows.

Proposition 3.1.8. *The group of unit quaternions is a subgroup of the group of non-zero quaternions ($S^3 \leq \mathbb{H}\backslash\{0\}$).*

Proof. To justify that $S^3 \leq \mathbb{H}\backslash\{0\}$ we need to check the three axioms of the subgroup criterion.

1. *Closure:* First we need to check that S^3 is closed under multiplication. If we have $q, r \in S^3$, then $qr \in S^3$ since $N(qr) = N(q)N(r) = 1$.

2. *Identity:* Second we check if the identity element of the group of non-zero quaternions is also in S^3. The identity element of $\mathbb{H}\backslash\{0\}$ is 1 which has norm 1 meaning that $1 \in S^3$.

3. *Inverses:* Finally we have got to check that we have $q^{-1} \in S^3$ for all $q \in S^3$. From the proof of Lemma 2.2.5 we know that $q^{-1} = \overline{q}N(q)^{-1}$. Therefore the inverse of q is just its conjugate since $N(q) = 1$. The norm of $\overline{q}$ is always the same as the norm of q since $N(q)$ is the sum of squares of the coefficients in q. Therefore $q^{-1} \in S^3$ for all $q \in S^3$.

Hence S^3 is a subgroup of $\mathbb{H}\backslash\{0\}$ since the three axioms of the subgroup criterion are satisfied. □

Note that the result from Proposition 3.1.8 will be very important later on in the project when we find the finite subgroups of the quaternions.

Definition 3.1.9 (Group of linear transformation of $\mathbb{H}$ [1])**.** $SL_4(\mathbb{R})$ is the *group of linear transformations* of $\mathbb{H}$ of determinant 1.

Note that the group of invertible linear transformations without any restrictions on the determinant is denoted $GL_4(\mathbb{R})$. Clearly, when $q \neq 0$, the functions $L(q)$ and $R(q)$ are in $GL_4(\mathbb{R})$ because they are $\mathbb{R}$-linear transformations. However, we do not know whether or not they are in $SL_4(\mathbb{R})$. In the following lemma, we will see that $L(q)$ and $R(q)$ are in $SL_4(\mathbb{R})$ if q is a unit quaternion.

Lemma 3.1.10. *The two restrictions of L to S^3 and R to S^3 are monomorphisms from S^3 into $SL_4(\mathbb{R})$.*

Proof. Firstly we need to check that if $q \in S^3$ then $L(q) \in SL_4(\mathbb{R})$. The norm of q is 1 and by Proposition 3.1.6, $N(q)^2 = \det L(q)$. Hence $\det L(q) = 1$ meaning that $L(q) \in SL_4(\mathbb{R})$ by definition. $R(q)$ is also in $SL_4(\mathbb{R})$ in the same way since $\det R(q) = \det L(q)$ by Proposition 3.1.6. Now note that a monomorphism is an injective homomorphism. So we have to check both of these properties are true.

1. *Homomorphism:* To show that this map is a homomorphism we need to show that $L(q_1q_2) = L(q_1)L(q_2)$ and $R(q_1q_2) = R(q_1)R(q_2)$ for all $q_1, q_2 \in S^3$. We have

$$L(q_1q_2)(h) = (q_1q_2)h = (q_1)(q_2h) = L(q_1)(L(q_2))(h),$$

and so $L(q_1q_2) = L(q_1)L(q_2)$. Then we have

$$R(q_1q_2)(h) = (h)(\overline{q_1q_2}) = (h\overline{q_1})(\overline{q_2}) = R(q_2)(R(q_1))(h),$$

and so $R(q_1q_2) = R(q_1)R(q_2)$. Therefore we have a homomorphism.

2. *Injective:* To show that this map is injective we check that the kernel is 1 ($\ker L = \ker R = \{1\}$). We have $\ker L = \{q \mid L(q) = id\}$. The statement $L(q) = id$ means that for all $h \in \mathbb{H}$ we have $L(q)(h) = h$ (i.e. $qh = h$). This must be true for all h, and in particular $h = 1$ for which we have $q1 = 1$, so $q = 1$. Therefore $\ker L = \{1\}$. Similarly, we have $\ker R = \{q \mid R(q) = id\}$. The statement $R(q) = id$ means that for all $h \in \mathbb{H}$ we have $R(q)(h) = h$ (i.e. $h\overline{q} = h$). This must be true for all h, and in particular $h = 1$ for which we have $1\overline{q} = 1$, so $\overline{q} = 1 \implies q = 1$ since the conjugate of 1 is still 1. Therefore $\ker R = \{1\}$.

Hence, the restrictions of L to S^3 and R to S^3 are monomorphisms from S^3 into $SL_4(\mathbb{R})$. □

Lemma 3.1.10 tells us that there exist maps, namely $L(q)$ and $R(q)$, from the group of unit quaternions, S^3, to the group of linear transformations of determinant 1, $SL_4(\mathbb{R})$, and that these maps are monomorphisms.

Next, we will show that there is a homomorphism from the cartesian product of S^3 with itself to $SL_4(\mathbb{R})$. To prove this we need to note that $L(q)$ and $R(q)$ commute for any $q, r \in \mathbb{H}$. This is true since $R(r)(L(q)h) = L(q)(R(r)h)$ shown as follows:

$$R(r)(L(q)h) = R(r)(qh) = qh\overline{r} \tag{3.1}$$

$$L(q)(R(r)h) = L(q)(h\overline{r}) = qh\overline{r}. \tag{3.2}$$

The commutativity of these linear transformations along with Lemma 3.1.10 helps us to prove the following proposition.

Proposition 3.1.11. *The map*

$$S^3 \times S^3 \to SL_4(\mathbb{R})$$
$$(q, r) \mapsto L(q)R(r)$$

is a homomorphism and its kernel is $\{(1, 1), (-1, -1)\}$.

Proof. Firstly we show that this is a homomorphism by checking that $L(q_1q_2)R(r_1r_2) = L(q_1)R(r_1)L(q_2)R(r_2)$ for $q_1, q_2, r_1, r_2 \in S^3$.

$$\begin{aligned} L(q_1q_2)R(r_1r_2) &= L(q_1)L(q_2)R(r_1)R(r_2) \quad \text{(since } L \text{ and } R \text{ are homomorphisms)} \\ &= L(q_1)R(r_1)L(q_2)R(q_2) \quad \text{(by commutativity of } L(q_2) \text{ and } R(r_1)\text{)}. \end{aligned}$$

Therefore the map is a homomorphism. Next we need to show that the kernel is $\{(1, 1), (-1, -1)\}$. We have that the kernel is given by

$$\begin{aligned} \{(q, r) \mid L(q)R(r) = id\} &= \{(q, r) \mid L(q)R(r)(h) = h, \forall h \in \mathbb{H}\} \\ &= \{(q, r) \mid qh\overline{r} = h, \forall h \in \mathbb{H}\}. \end{aligned}$$

This must be true for all h, in particular $h = 1$ for which $q\overline{r} = 1$. So $\overline{r} = q^{-1} = \frac{\overline{q}}{N(q)} = \frac{\overline{q}}{1} \implies r = q$. If $q \in \mathbb{R}$ then $N(q) = 1$ means that $q^2 = 1$ so q is either 1 or -1. Since $r = q$ we have that $qh\overline{r} = qh\overline{q} = h \implies qhq^{-1} = h \implies qh = hq$ for all $h \in \mathbb{H}$. This means that q must be central in $\mathbb{H}$ because it commutes with every element in $\mathbb{H}$. By Proposition 2.1.8 the centre of the quaternions, $Z(\mathbb{H})$, is $\mathbb{R}$, thus q must be a real number. Therefore q can only be 1 or -1 and since $r = q$, the kernel is $\{(-1, -1), (1, 1)\}$. □

In the previous two propositions we have shown that there is a homomorphism from the group of unit quaternions to the group of linear transformations of $\mathbb{H}$ with determinant 1. We already proved that S^3 is a subgroup of the group of non-zero quaternions in Proposition 3.1.8. These results will be useful for us in the next section when constructing homomorphisms from S^3 to other groups.

To end this section we will prove the following proposition which gives three equivalent properties of two elements $q, r \in \mathbb{H}$. The equivalence of these properties will be very useful for proving later results in this chapter.

Proposition 3.1.12. *For non-zero elements $q, r \in \mathbb{H}$, the following are equivalent:*

(i) q and r have the same norm and trace,

(ii) $q = hrh^{-1}$ for some $h \in S^3$,

(iii) $N(q)$ is an eigenvalue of $L(q)R(r)$.

Proof. By letting $q = hrh^{-1}$ we can compute the norm of q as follows:

$$\begin{aligned} N(q) = N(hrh^{-1}) &= N(h)N(r)N(h^{-1}) && \text{(by Proposition 2.3.5(iii))} \\ &= 1 \times N(r) \times 1 && (\text{since } h \in S^3) \\ &= N(r). \end{aligned}$$

We can also compute the trace of q similarly:

$$\begin{aligned} Tr(q) = Tr(hrh^{-1}) &= Tr(h^{-1}hr) && \text{(by Proposition 2.3.5(v))} \\ &= Tr(r). \end{aligned}$$

Hence we have $N(q) = N(r)$ and $Tr(q) = Tr(r)$ for $q, r \in \mathbb{H}$. Therefore (ii) implies (i).

Now suppose that q and r have the same norm and trace. If $q \in \mathbb{R}$, let $r = a+bi+cj+dk$ where $a, b, c, d \in \mathbb{R}$. Then $Tr(r) = 2a = Tr(q) = 2q$ since q is real, so $q = a$. Now $N(q) = a^2$ and $N(r) = a^2 + b^2 + c^2 + d^2 \implies b = c = d = 0$ since q and r have the same norm. Therefore $r = q$. In this case, we may take $h = 1$ so that both (ii) and (iii) are satisfied.

If $q \notin \mathbb{R}$, we regard $\mathbb{H}$ as a 2-dimensional vector space over $K := \mathbb{R}[q]$. Then $R(r)$ is a K-linear transformation because $R(r)$ commutes with left multiplication by $a + bq$ where $a, b \in \mathbb{R}$ (by equations 3.1 and 3.2). The eigenvalues of $R(r)$ are the roots of $x^2 - Tr(r)x + N(r) = 0$ in K, calculated as follows:

$$\begin{aligned} x &= \frac{Tr(r) \pm \sqrt{Tr(r)^2 - 4N(r)}}{2} \\ &= \frac{q + \overline{q} \pm \sqrt{(q + \overline{q})^2 - 4r\overline{q}}}{2} && (\text{Since } N(r) = N(q) \text{ and } Tr(r) = Tr(q)) \\ &= \frac{q + \overline{q} \pm \sqrt{q^2 + \overline{q}^2 - 2q\overline{q}}}{2} \\ &= \frac{q + \overline{q} \pm \sqrt{(q - \overline{q})^2}}{2} \\ &= \frac{q + \overline{q} \pm (q - \overline{q})}{2} \\ \implies x &= \frac{q + \overline{q} + q - \overline{q}}{2} = q, \text{ or } \quad x = \frac{q + \overline{q} - q + \overline{q}}{2} = \overline{q}. \end{aligned}$$

The matrix $R(r)$ satisfies the equation $x^2 - Tr(r)x + N(r) = 0$ because r does. If $h \in S^3$ is an eigenvector of norm 1 corresponding to $\overline{q}$, then $h\overline{r} = \overline{q}h$ and so $q = hrh^{-1}$

and (i) implies (ii). On the other hand,

$$\begin{aligned} h\overline{r} = \overline{q}h &\iff h\overline{r} = \frac{N(q)}{q}h \qquad\qquad (\text{Since } \overline{q} = \frac{N(q)}{q}) \\ &\iff qh\overline{r} = N(q)h \\ &\iff L(q)R(r)h = N(q)h, \end{aligned}$$

and so (ii) implies (iii) and (iii) implies (ii).
Hence we have shown that (i) $\iff$ (ii) $\iff$ (iii) and so they are all equivalent. □

3.2 Pure Quaternions and Orthogonal Groups

Continuing on from what we saw in the previous section, we will now construct homomorphisms from the group of unit quaternions to other groups, namely the groups of orthogonal transformations. We will also define the pure quaternions and find out about their relationship with the orthogonal groups. Note that pure quaternions do not form a group and we will discuss why this is the case.

The norm function $N(q)$ is the square of the usual Euclidean distance in $\mathbb{H}$ regarded as $\mathbb{R}^4$. The associated Euclidean inner product is

$$q \cdot r = \frac{1}{2}Tr(q\overline{r}). \tag{3.3}$$

The basis $\{1, i, j, k\}$ is orthonormal with respect to this inner product.

Example 3.2.1. To show that the basis $\{1, i, j, k\}$ is orthonormal we use the inner product (equation 3.3) and check that $q \cdot r = 0$ for all basis elements, $q \neq r$. For example, for $q = i$ and $r = j$ we have

$$\begin{aligned} i \cdot j = \frac{1}{2}Tr(i\overline{j}) = \frac{1}{2}Tr(-ij) = \frac{1}{2}Tr(-k) &= \frac{1}{2}(-k + (-\overline{k})) \\ &= \frac{1}{2}(-k + k) = 0, \end{aligned}$$

as required. To show the basis is orthonormal we check that $q \cdot q = 1$ for all basis elements. For example, for $q = i$ we have

$$i \cdot i = \frac{1}{2}Tr(i\overline{i}) = \frac{1}{2}Tr(-i^2) = \frac{1}{2}Tr(1) = \frac{1}{2}(1 + \overline{1}) = 1.$$

This example shows us that the basis $\{1, i, j, k\}$ of $\mathbb{H}$ is orthonormal meaning that it spans the quaternions. This leads us to the following definition of a certain subspace of the quaternions.

Definition 3.2.2 (Pure quaternions [1])**.** The set of *pure quaternions* is the subspace V of the quaternions and is spanned by i, j, k.

In other words, an element $q \in \mathbb{H}$ given by $q = a + bi + cj + dk$ (where $a, b, c, d \in \mathbb{R}$) is a pure quaternion if and only if $a = 0$. So $q \in V$ if and only if $q = bi + cj + dk$. Note that unlike the unit quaternions, S^3, we have defined the pure quaternions as a subspace of the quaternion algebra and not as a subgroup of $\mathbb{H}\backslash\{0\}$. This is because V is not a group and this is clear since there is no identity element (since $1 \notin V$). In fact, we will prove the relationship between V and 1 in the following lemma.

Lemma 3.2.3. *V is the orthogonal complement of 1 and we have that $q \in V$ if and only if $q^2 \in \mathbb{R}$ and $q^2 \leq 0$.*

Proof. To show that v is the orthogonal complement of 1 we need to show that every element in V is orthogonal to 1 and vice versa. Let $q = bi + cj + dk$ be an arbitrary element in V where $b, c, d \in \mathbb{R}$. The inner product of q and 1 is

$$q \cdot 1 = \begin{pmatrix} 0 \\ b \\ c \\ d \end{pmatrix} \cdot \begin{pmatrix} 1 \\ 0 \\ 0 \\ 0 \end{pmatrix} = 0.$$

Also, if $a + bi + cj + dk$ is orthogonal to 1 then a must be equal to zero which implies that $a + bi + cj + dk \in V$. Hence V is the orthogonal complement of 1.

Next, we need to show both directions of the second statement. First, we show that $q \in V \implies q^2 \in \mathbb{R}$ and $q^2 \leq 0$. As before, let $q = bi + cj + dk$ with $b, c, d \in \mathbb{R}$ be an arbitrary element in V. Then

$$\begin{aligned} q^2 &= (bi + cj + dk)(bi + cj + dk) \\ &= b^2i^2 + bcij + bcji + c^2j^2 + cdjk + cdkj + d^2k^2 \\ &= b^2i^2 + c^2j^2 + d^2k^2 && \text{(since } ji = -ij \text{ and } kj = -jk) \\ &= -b^2 - c^2 - d^2 && \text{(since } i^2 = j^2 = k^2 = -1). \end{aligned}$$

Since $b, c, d \in \mathbb{R}$, we have $q^2 \in \mathbb{R}$. Moreover, $q^2 = -b^2 - c^2 - d^2 = -(b^2 + c^2 + d^2) \leq 0$ since the sum of the squares of real numbers is always non-negative and we have the negation of this.
Now we show that $q^2 \in \mathbb{R}$ and $q^2 \leq 0 \implies q \in V$. Assume for a contradiction that $q = a + r$ where $r \in V$ and $a \in \mathbb{R} \backslash \{0\}$ (i.e. $q \notin V$). Then $q^2 = (a+r)^2 = a^2 + r^2 + 2ar$. Clearly $a^2 \in \mathbb{R}$ and we have already shown that $r \in V \implies r^2 \in \mathbb{R}$. However, if $a \neq 0$ and $r \neq 0$ then the term $2ar$ is clearly in V meaning that $q^2 \notin \mathbb{R}$, which is a contradiction. Therefore we cannot have the $2ar$ term if $q^2 \in \mathbb{R}$, so we can have either $q^2 = a^2$ or $q^2 = r^2$. We also have that $q^2 \leq 0$ but this is not possible for $q^2 = a^2$ where $a \in \mathbb{R} \backslash \{0\}$. This contradicts our assumption that $a \neq 0$. Therefore a must be zero and we have $q \in V$ as required. □

Remember the fact that $q^2 = -b^2 - c^2 - d^2$ for all $q \in V$ given by $q = bi + cj + dk$ as it will be useful for proving later results.

Any non-zero $\mathbb{R}$-linear transformation of a Euclidean space is orthogonal if and only if it preserves the inner product. So if M is a matrix for a linear transformation T with respect to an orthonormal basis, then T is orthogonal if and only if M is an orthogonal matrix ($MM^T = M^T M = I$ where M^T is the transpose of the matrix M). Hence if M is orthogonal, then $(\det M)^2 = 1$, which means that the determinant of an orthogonal transformation $\det M$ is either 1 or -1. In terms of the dot product, T is orthogonal if and only if $T(u) \cdot T(v) = u \cdot v$ for all $u, v \in \mathbb{R}^n$.

Now we will define the groups of orthogonal transformations of quaternions.

Definition 3.2.4 (Orthogonal Groups [1])**.** The set of orthogonal transformations of $\mathbb{H}$ is the *orthogonal group* $O_4(\mathbb{R})$. The subgroup of $O_4(\mathbb{R})$ which consists of the orthogonal transformations of determinant 1 is called the *special orthogonal group* $SO_4(\mathbb{R})$. The elements of $SO_4(\mathbb{R})$ are called *rotations*.

Remark Similarly, the orthogonal transformations of pure quaternions V constitute the orthogonal group $O_3(\mathbb{R})$ and such transformations with determinant 1 are in the special orthogonal group $SO_3(\mathbb{R})$.

Soon we are going to be able to prove that the linear transformations $L(q)$ and $R(q)$ defined in the previous chapter are also orthogonal transformations when q is a unit quaternion. However, we will need the following result to help prove this.

Lemma 3.2.5. *For a linear transformation $T : \mathbb{R}^n \to \mathbb{R}^n$ the following are equivalent:*

(i) T is orthogonal,

(ii) $T(v) \cdot T(v) = v \cdot v$ for all $v \in \mathbb{R}^n$.

Proof. Assume that T is an orthogonal transformation. By definition, for any $v, u \in \mathbb{R}^n$ we have $T(v) \cdot T(u) = v \cdot u$. Now take $u = v$. Then we get $T(v) \cdot T(v) = v \cdot v$ for all $v \in \mathbb{R}^n$ and we have shown (i) implies (ii).
Now assume part (ii) of the Lemma. Let $u, v \in \mathbb{R}^n$. We want to show that $T(u) \cdot T(v) = u \cdot v$. Since T is bilinear we have that $(u + v) \cdot (u + v) = u \cdot u + 2u \cdot v + v \cdot v$ which we rearrange to get

$$u \cdot v = \frac{1}{2}((u + v) \cdot (u + v) - u \cdot u - v \cdot v).$$

By our assumption of part (ii), we have $(u + v) \cdot (u + v) = T(u + v) \cdot T(u + v)$, $u \cdot u = T(u) \cdot T(u)$, and $v \cdot v = T(v) \cdot T(v)$. Thus, we get

$$\begin{aligned} u \cdot v &= \frac{1}{2}((u + v) \cdot (u + v) - u \cdot u - v \cdot v) \\ &= \frac{1}{2}(T(u + v) \cdot T(u + v) - T(u) \cdot T(u) - T(v) \cdot T(v)) \\ &= T(u) \cdot T(v). \end{aligned}$$

Hence T is an orthogonal transformation and we have shown that (ii) implies (i). □

Now by using Lemma 3.2.5, we can prove that $L(q)$ and $R(q)$ are in $SO_4(\mathbb{R})$, which is an important result as it shows that there exists a map from S^3 to $SO_4(\mathbb{R})$.

Corollary 3.2.6. *For $q \in S^3$, the linear transformations $L(q)$ and $R(q)$ belong to $SO_4(\mathbb{R})$.*

Proof. An element of the special orthogonal group $SO_4(\mathbb{R})$ is a transformation that is both orthogonal and linear with determinant 1. Hence we have

$$SO_4(\mathbb{R}) = O_4(\mathbb{R}) \cap SL_4(\mathbb{R}).$$

We already know that for $q \in S^3$, $L(q)$ and $R(q)$ belong to $SL_4(\mathbb{R})$ by Lemma 3.1.10. Thus we only need to show that $L(q), R(q) \in O_4(\mathbb{R})$.
Let $h \in \mathbb{H}$. Then we have

$$\begin{aligned} N(L(q)h) = N(qh) &= N(q)N(h) && \text{(By Proposition 2.3.5(iii))} \\ &= N(h) && (N(q) = 1 \text{ since } q \in S^3). \end{aligned}$$

Since $N(L(q)h) = N(h)$, then we must have that $L(q)h \cdot L(q)h = h \cdot h$. Thus $L(q)$ is orthogonal by Lemma 3.2.5.
Similarly, we have

$$\begin{aligned} N(R(q)h) = N(h\overline{q}) &= N(h)N(\overline{q}) && \text{(By Proposition 2.3.5(iii))} \\ &= N(h)N(q) && (\text{Since } N(\overline{q}) = N(q)) \\ &= N(h) && (N(q) = 1 \text{ since } q \in S^3). \end{aligned}$$

Since $N(R(q)h) = N(h)$, then we must have that $R(q)h \cdot R(q)h = h \cdot h$. Thus $R(q)$ is orthogonal by Lemma 3.2.5.
Thus we have shown that $L(q)$ and $R(q)$ belong to both $O_4(\mathbb{R})$ and $SL_4(\mathbb{R})$. Therefore they both belong to $SO_4(\mathbb{R})$. $\square$

By Lemma 3.1.10, $L(q)$ and $R(q)$ are monomorphisms form S^3 into $SL_4(\mathbb{R})$, the group of linear transformations of $\mathbb{H}$ of determinant 1. Corollary 3.2.6 has now extended this to a monomorphism from S^3 into $SO_4(\mathbb{R})$.

The next aim is to show that there also exists a homomorphism from S^3 into $SO_3(\mathbb{R})$, the group of orthogonal transformations of pure quaternions with determinant 1. Before we prove this result we need to construct another linear transformation as follows.

Definition 3.2.7. For $q \in S^3$, the linear transformation $B(q)$ of V is given by $B(q)(v) := qvq^{-1} = L(q)R(q)(v)$ where $v \in V$.

Now we will show that when v is a pure quaternion, then $B(q)(v)$ is also a pure quaternion.

Lemma 3.2.8. $v \in V \implies qvq^{-1} \in V$.

Proof. Let $q \in S^3$ and $v \in V$. Then $(qvq^{-1})^2 = qvq^{-1}qvq^{-1} = qv^2q^{-1}$. From the proof of Lemma 3.2.3 we have seen that $v \in V \Leftrightarrow v^2 \in \mathbb{R}_{\leq 0}$, and so v^2 is central in $\mathbb{H}$ by Proposition 2.1.8. Therefore $(qvq^{-1})^2 = qv^2q^{-1} = qq^{-1}v^2 = v^2 \in \mathbb{R}_{\leq 0}$. Hence $qvq^{-1} \in V$ by Lemma 3.2.3. □

In the next proposition we prove that $B(q)$ is in $SO_3(\mathbb{R})$ and this will be very important to us when we prove that there is a homomorphism from S^3 into $SO_3(\mathbb{R})$ since $B(q)$ will be the map between the two groups.

Proposition 3.2.9. *For $q \in S^3$ we have $B(q) \in SO_3(\mathbb{R})$.*

Proof. Let $q \in S^3$. Firstly we have that

$$\begin{aligned} N(B(q)v) = N(qvq^{-1}) &= N(qv\overline{q}) && (\text{Since } \overline{q} = q^{-1} \text{ for } q \in S^3) \\ &= N(q)N(v)N(q^{-1}) && (\text{By Proposition 2.3.5(iii)}) \\ &= N(v) && (N(q) = N(\overline{q}) = 1) \end{aligned}$$

which implies that $B(q)v \cdot B(q)v = v \cdot v$. So $B(q) \in O_3(\mathbb{R})$ by Lemma 3.2.5.
It remains to show that $B(q)$ has determinant 1. Let $\mathcal{B} = \{1, i, j, k\}$ be a basis of $\mathbb{H}$. We have that $q1q^{-1} = qq^{-1} = 1$, so if $h \in \mathbb{H}$, then we have that the matrix of $[h \mapsto qhq^-1]_{\mathcal{B}}$ is given by

$$\begin{pmatrix} 1 & - & - & - \\ 0 & * & * & * \\ 0 & * & * & * \\ 0 & * & * & * \end{pmatrix}$$

where $*$ represents coefficients of i, j, k for $B(q)i, B(q)j, B(q)k$. Due to cancellation, the determinant of this matrix must be given by the determinant of the 3×3 submatrix in the bottom right (represented by $*$). By definition, this submatrix is equivalent to the matrix of $B(q)$.
On the other hand the map $h \mapsto qhq^{-1}$ on $\mathbb{H}$ is the same as $L(q)R(q)$. Therefore we

have that

$$\begin{aligned}
\det B(q) &= \det[h \mapsto qhq^{-1}]_{\mathcal{B}} \\
&= \det L(q)R(q) \\
&= \det L(q) \det R(q) \\
&= N(q)^2 N(q)^2 && \text{(By Proposition 3.1.6)} \\
&= 1 && \text{(Since } q \in S^3\text{).}
\end{aligned}$$

Hence $B(q) \in SO_3(\mathbb{R})$. □

Since $B(q) \in SO_3(\mathbb{R})$ we can show that $B(q)$ defines a homomorphism from the unit quaternions to $SO_3(\mathbb{R})$. The maps $L(q)$ and $R(q)$ from S^3 to $SO_4(\mathbb{R})$ were monomorphisms. However, in this case $B(q)$ from S^3 to $SO_3(\mathbb{R})$ is not injective because it has a kernel $\{-1, 1\}$. However, unlike the monomorphisms from S^3 to $SO_4(\mathbb{R})$, this homomorphism is surjective, so we call it an epimorphism. We will prove this in the following proposition.

Proposition 3.2.10. *The map $B\colon S^3 \to SO_3(\mathbb{R})$ is a homomorphism onto $SO_3(\mathbb{R})$ with kernel $\{-1, 1\}$.*

Proof. We show that B is a homomorphism by checking that $B(q_1q_2)v = B(q_1)B(q_2)v$ where $q_1, q_2 \in S^3$.

$$\begin{aligned}
B(q_1q_2)v &= L(q_1q_2)R(q_1q_2)v \\
&= L(q_1)L(q_2)R(q_1)R(q_2)v && \text{(Since } L \text{ and } R \text{ are homomorphisms)} \\
&= L(q_1)R(q_1)L(q_2)R(q_2)v && \text{(By commutativity of } L(q_2) \text{ and } R(q_1)\text{)} \\
&= B(q_1)B(q_2)v.
\end{aligned}$$

Hence $B : S^3 \to SO_3(\mathbb{R})$ is a homomorphism. The kernel of B is given by

$$\begin{aligned}
\ker B &= \{q \mid L(q)R(q)v = v\} \\
&= \{q \mid qvq^{-1} = v, \forall v \in V\}.
\end{aligned}$$

If $qvq^{-1} = v$ for all $v \in V$, then q commutes with all pure quaternions and so q commutes with the whole of $\mathbb{H}$. By Proposition 2.1.8, this means that $q \in \mathbb{R}$ because $Z(\mathbb{H}) = \mathbb{R}$. So $\ker B = S^3 \cap \mathbb{R} = \{-1, 1\}$ (since $q = -1$ and $q = 1$ are the only real numbers where $N(q) = q\overline{q} = 1$).

Now we need to show that B is surjective. Suppose that we have a transformation $T \in SO_3(\mathbb{R})$. By Proposition 3.1.12, there exists $h \in S^3$ such that $B(h)T(i) = i$. We have that $Tr(T(i)) = Tr(i) = 0$ because all pure quaternions have trace zero. We also have $N(T(i)) = N(i)$ because $T \in O_3(\mathbb{R})$ is an orthogonal transformation. Since $T(i)$ and i have the same norm and trace, then $T(i) = hih^{-1}$ by Proposition 3.1.12(ii). This is equivalent to $B(h)T(i) = i$ by Definition 3.2.7.

Replacing T by $B(h)T$ we may suppose that $T(i) = i$. Then $T(j)$ is orthogonal to i as $T \in O_3(\mathbb{R})$. So we can write $T(j) = \alpha j$ for some $\alpha \in \mathbb{C}$ (since $\alpha j = (a+bi)j = aj + bk$ for some $a, b \in \mathbb{R}$). Choose $\beta \in \mathbb{C}$ such that $\alpha = \beta^2$. Then observe that

$$\begin{aligned} B(\beta)j = \beta j \overline{\beta} &= \beta^2 j && \text{(Since } j\overline{\beta} = \beta j\text{)} \\ &= \alpha j = T(j). \end{aligned}$$

Thus $B(\beta)^{-1}T$ fixes i and j meaning that $k = ij$ is also fixed. Since $B(\beta)^{-1}T$ is orthogonal and of determinant 1 it must be the identity because

$$\begin{aligned} B(\beta)^{-1}T(i) &= i \\ B(\beta)^{-1}T(j) &= j \implies B(\beta)^{-1}T = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} = I. \\ B(\beta)^{-1}T(k) &= k \end{aligned}$$

Thus $B(\beta)^{-1}T = I \implies T = B(\beta)$ meaning that B must be surjective. $\square$

Note that the centre of $O_3(\mathbb{R})$ is $\langle -I \rangle$, where I is the identity transformation and since $\det(-I) = -1$ we get

$$O_3(\mathbb{R}) = \langle -I \rangle \times SO_3(\mathbb{R}) = \langle -I \rangle \times S^3/\{-1, 1\}.$$

This follows from the fact that $O_3(\mathbb{R})$ consists of all orthogonal transformations of V of with determinant -1 or 1 whilst $SO_3(\mathbb{R})$ only consists of those of determinant 1. It also follows from Proposition 3.2.10 that $SO_3(\mathbb{R}) = S^3/\{-1, 1\}$.

Rotations Since $N(q) = 1$ for $q \in S^3$, we can write $q = a + bu$ for some $u \in V$ such that $N(u) = 1$ and for some $a, b \in \mathbb{R}$ such that $a^2 + b^2 = 1$. Now let $a = \cos \frac{1}{2}\theta$ and let $b = \sin \frac{1}{2}\theta$ so that $q = \cos \frac{1}{2}\theta + u \sin \frac{1}{2}\theta$. Then $B(q)$ is a rotation through angle θ about axis u. To see that this is the case we have the following proposition.

Proposition 3.2.11. *Suppose u is a unit vector in V and $v \in V$ is a unit vector orthogonal to u. Then $\{u, v, \frac{1}{2}(uv - vu)\}$ is an orthonormal basis of V, and the matrix of $B(q)$ with respect to this basis is*

$$B(q) = \begin{pmatrix} 1 & 0 & 0 \\ 0 & \cos\theta & -\sin\theta \\ 0 & \sin\theta & \cos\theta \end{pmatrix}.$$

Proof. We first need to show that $u, v, \frac{1}{2}(uv - vu)$ is an orthonormal basis. We assume that u and v are unit vectors and orthogonal to each other so we need to show that u and v are both orthogonal to $\frac{1}{2}(uv - vu)$ and that $\frac{1}{2}(uv - vu)$ is a unit vector. Since u and v are pure quaternions, $\overline{u} = -u$ and $\overline{v} = -v$. Hence $N(u) = u\overline{u} = u(-u) = -u^2$ and similarly $N(v) = -v^2$. Since u and v are unit vectors, $N(u) = N(v) = 1$ which implies that $u^2 = v^2 = -1$. From the proof of Lemma 3.2.5 we have that

$$\begin{aligned} u \cdot v &= \frac{1}{2}((u + v) \cdot (u + v) - u \cdot u - v \cdot v) \\ &= \frac{1}{2}(N(u + v) - N(u) - N(v)) \\ &= \frac{1}{2}(|u + v|^2 - |u|^2 - |v|^2) \end{aligned}$$

and since $|u|^2 = N(u) = -u^2$, $|v|^2 = N(v) = -v^2$ and $|u+v|^2 = N(u+v) = -(u+v)^2$, we can write

$$\begin{aligned} u \cdot v &= \frac{1}{2}(-(u + v)^2 + u^2 + v^2) \\ &= \frac{1}{2}(-(u^2 + uv + vu + v^2) + u^2 + v^2) \\ &= \frac{1}{2}(-uv - vu) \\ &= -\frac{1}{2}(uv + vu). \end{aligned}$$

So we have obtained the formula $u \cdot w = -\frac{1}{2}(uw + wu)$ whenever u, w are vectors in V. Hence, if we let $w = \frac{1}{2}(uv - vu)$ we get

$$\begin{aligned} u \cdot \frac{1}{2}(uv - vu) &= -\frac{1}{2}\left(u\left(\frac{1}{2}(uv - vu)\right) + \left(\frac{1}{2}(uv - vu)\right)u\right) \\ &= -\frac{1}{4}(uuv - uvu + uvu - vuu) \\ &= -\frac{1}{4}(u^2v - vu^2) \\ &= -\frac{1}{4}(-v + v) && \text{(Since } u^2 = -1\text{)} \\ &= 0 \end{aligned}$$

as required. In a similar way we get $v \cdot \frac{1}{2}(uv - vu) = 0$ meaning that $u, v, \frac{1}{2}(uv - vu)$ are orthogonal. Now we need to show that $\frac{1}{2}(uv - vu)$ is a unit vector (i.e. $N\left(\frac{1}{2}(uv - vu)\right) = 1$. Note that we have obtained that $u \cdot v = -\frac{1}{2}(uv + vu)$ when u, v are unit vectors. Since u and v are orthogonal, we have that $u \cdot v = -\frac{1}{2}(uv + vu) = 0$. Hence we have that $uv = -vu$. Now we can calculate the norm of $\frac{1}{2}(uv - vu)$ as follows:

$$\begin{aligned} N\left(\frac{1}{2}(uv - vu)\right) &= -\left(\frac{1}{2}(uv - vu)\right)^2 \\ &= -\frac{1}{4}(uvuv - uvvu - vuuv + vuvu) \\ &= -\frac{1}{4}(uvuv + u^2 + v^2 + vuvu). \end{aligned}$$

Since $u^2 = v^2 = -1$, the above is equal to

$$\begin{aligned} N\left(\frac{1}{2}(uv - vu)\right) &= -\frac{1}{4}(uvuv - 2 + vuvu) \\ &= -\frac{1}{4}(-vuuv - 2 - vvuu) && \text{(Since } uv = -vu) \\ &= -\frac{1}{4}(-1 - 2 - 1) && \text{(Since } u^2 = v^2 = -1) \\ &= 1 \end{aligned}$$

as required. Thus we have shown that $u, v, \frac{1}{2}(uv - vu)$ is an orthonormal basis of V. Now we can calculate the matrix of $B(q)$ with respect to this orthonormal basis. Firstly we calculate $B(q)u$ as follows:

$$\begin{aligned} B(q)u &= qu\bar{q} \\ &= (a + bu)u(a - bu) \\ &= (au + bu^2)(a - bu) \\ &= a^2u - abu^2 + abu^2 - b^2u^3 \\ &= (a^2 + b^2)u && \text{(Since } u^2 = -1) \\ &= u && \text{(Since } a^2 + b^2 = 1). \end{aligned}$$

Then we get

$$\begin{aligned}
B(q)v &= qv\overline{q} \\
&= (a+bu)v(a-bu) \\
&= (av+buv)(a-bu) \\
&= a^2v + abuv - abvu - b^2uvu \\
&= a^2v + ab(uv-vu) + b^2vu^2 && \text{(Since } uv = -vu\text{)} \\
&= (a^2-b^2)v + 2ab\left(\frac{1}{2}(uv-vu)\right) && \text{(Since } u^2 = -1\text{).}
\end{aligned}$$

Now note the trigonometric identities $\sin^2\theta + \cos^2\theta = 1$ and $\cos 2\theta = 2\cos^2\theta - 1$. Then using these identities we get

$$\begin{aligned}
a^2 - b^2 &= \cos^2\frac{1}{2}\theta - \sin^2\frac{1}{2}\theta \\
&= \cos^2\frac{1}{2}\theta - (1 - \cos^2\frac{1}{2}\theta) \\
&= 2\cos^2\frac{1}{2}\theta - 1 \\
&= \cos\theta.
\end{aligned}$$

Note another trigonometric identity that $\sin\theta_1\cos\theta_2 = \frac{1}{2}(\sin(\theta_1+\theta_2) + \sin(\theta_1-\theta_2))$. Then using this identity we get

$$\begin{aligned}
2ab &= 2\left(\cos\frac{1}{2}\theta\sin\frac{1}{2}\theta\right) \\
&= 2\left(\frac{1}{2}\left(\sin\left(\frac{\theta}{2}+\frac{\theta}{2}\right) + \sin\left(\frac{\theta}{2}-\frac{\theta}{2}\right)\right)\right) \\
&= \sin\theta + \sin 0 \\
&= \sin\theta.
\end{aligned}$$

Hence $B(q)v = (\cos\theta)v + (\sin\theta)\frac{1}{2}(uv-vu)$. Then

$$\begin{aligned}
B(q)\frac{1}{2}(uv-vu) &= (a+bu)\frac{1}{2}(a-bu) \\
&= \frac{1}{2}(auv - avu) + bu^2v - buvu)(a-bu) \\
&= \frac{1}{2}(auv - avu - bv - buvu)(a-bu) \\
&= \frac{1}{2}(a^2uv - a^2vu - abv - abuvu - abuvu + abvuu + b^2vu + b^2uvuu).
\end{aligned}$$

Since we have that $u^2 = v^2 = -1$ and $uv = -vu$, we can simplify this as follows:

$$\begin{aligned}
B(q)\frac{1}{2}(uv - vu) &= \frac{1}{2}(a^2(uv - vu) - abv - abv - abv - abv + b^2vu - b^2uv) \\
&= \frac{1}{2}((a^2 - b^2)(uv - vu) - 4abv) \\
&= -2abv + (a^2 - b^2)\frac{1}{2}(uv - vu) \\
&= (-\sin\theta)v + (\cos\theta)\frac{1}{2}(uv - vu)
\end{aligned}$$

by the trigonometric identities we have used above. These calculations result in the matrix of $B(q)$ given by

$$\begin{pmatrix} 1 & 0 & 0 \\ 0 & \cos\theta & -\sin\theta \\ 0 & \sin\theta & \cos\theta \end{pmatrix}$$

as required. □

Proposition 3.2.11 shows that $B(q)$ is a rotation through angle θ about axis u because its matrix with respect to the orthonormal basis is the rotation matrix in 3 dimensions. The fact that $B(q)$ can represent a rotation will be very important later in the project.

We have seen that $B(q)$ can represent a rotation. Now we will see that with certain restrictions it can also represent a reflection. To do this first we will define the intersection of the pure quaternions and the unit quaternions.

Definition 3.2.12. The set $S^2 := V \cap S^3 = \{u \in V \mid u^2 = -1\}$ is a 2-sphere in V.

We can see that $S^2 = V \cap S^3 = \{u \in V \mid u^2 = -1\}$ is a 2-sphere by letting $u = bi + cj + dk$ where $b, c, d \in \mathbb{R}$. We saw previously that $u^2 = -(b^2 + c^2 + d^2)$ and since this is equal to -1 we have that $b^2 + c^2 + d^2 = 1$, the equation of a unit 2-sphere.

We can now restrict $B(q)$ to $B(u)$ where $u \in S^2$ so that we can get a formula for reflection.

Lemma 3.2.13. *If $u \in S^2$, then $-B(u)v = uvu = v - 2(u \cdot v)u$ is the reflection in the plane orthogonal to u.*

Proof. Clearly we have $-B(u)v = -(uv\overline{u}) = -(uv(-u)) = uvu$, since $\overline{u} = -u$ because $u \in V$. So we need to show that $uvu = v - 2(u \cdot v)u$. Firstly, we have seen from the proof of Proposition 3.2.11 that for $u \in V$ we have

$$u \cdot v = \frac{1}{2}(-(u+v)^2 + u^2 + v^2) = \frac{1}{2}(-uv - vu).$$

So we can rewrite uvu as

$$\begin{aligned} uvu &= -2\left(\frac{1}{2}(-uv - vu)\right)u - vu^2 \\ &= -2\left(\frac{1}{2}(-uv - vu)\right)u + v \qquad\qquad \text{(Since } u^2 = -1\text{)} \\ &= v - 2(u \cdot v)u \end{aligned}$$

as required. Since $u \cdot u = N(u) = 1$, we have $-B(u)v = v - 2\frac{u \cdot v}{u \cdot u}u$ which is the formula for the reflection $Ref_u(v)$ by Definition 3.1.2. $\square$

We can use our new formula for a reflection in terms of $B(u)$ with $u \in S^2$ to define reflection in $O_3(\mathbb{R})$ in the following proposition.

Proposition 3.2.14. *The element $r \in O_3(\mathbb{R})$ is a reflection if and only if $r = -B(u)$ for some $u \in S^2$.*

Proof. Any reflection in $O_3(\mathbb{R})$ must have order 2 and if r is a reflection, then $\det r = -1$. Thus $-r \in SO_3(\mathbb{R})$ (since $\det(-r) = 1$) and we can write $-r = B(u)$ for some $u \in S^3$, by Proposition 3.2.9. Hence we have $r = -B(u)$. An element of this form has order two if and only if $u^2 = \pm 1$. If $u^2 = 1$, then $u = \pm 1 \notin V$. So the element is a reflection if and only if $u^2 = -1$. Therefore we must have $u \in S^2$. $\square$

In Section 3.1 we saw that there is a homomorphism from the cartesian product of S^3 with itself to $SL_4(\mathbb{R})$ with kernel $\{(1,1),(-1,-1)\}$. We know straight away from this that $S^3 \times S^3 \to SO_4(\mathbb{R})$ is also a homomorphism with the same kernel. However, in the following proposition, we will show that this homomorphism is also surjective.

Proposition 3.2.15. *The map*

$$\begin{aligned} S^3 \times S^3 &\to SO_4(\mathbb{R}) \\ (q,r) &\mapsto L(q)R(r) \end{aligned}$$

is a homomorphism onto $SO_4(\mathbb{R})$ with kernel $\{(1,1),(-1,-1)\}$.

Proof. For $q, r \in S^3$, we already know that $(q, r) \mapsto L(q)R(r)$ is a homomorphism with kernel $\{(1, 1), (-1, -1)\}$ by Proposition 3.1.11. We also know that $L(q), R(r) \in SO_4(\mathbb{R})$ by Corollary 3.2.6, which implies that $L(q)R(r) \in SO_4(\mathbb{R})$. So all we need to show is that the map is surjective.
Suppose that $T \in SO_4(\mathbb{R})$ and set $q := T(1)$. Then $N(q) = 1$ and so $R(q)T$ fixes 1 and hence acts on V as an element of $SO_3(\mathbb{R})$. By Proposition 3.2.9 we can find $h \in S^3$ such that $R(q)T = B(h) = L(h)R(h)$. Thus $T = L(h)R(q^{-1}h)$ has the required form. □

To summarise, in this section we have used the fact that there is a homomorphism from the group S^3 to $SL_4(\mathbb{R})$ and extended this to $SO_4(\mathbb{R})$, the special group of orthogonal transformations of $\mathbb{H}$, by showing that $L(q)$ and $R(q)$ are orthogonal. We also defined the set of pure quaternions, V, and used them to define the linear transformation $B(q)$ and showed that $B(q)$ is orthogonal. Using $B(q)$ we were able to show that there was also a homomorphism from S^3 to $SO_3(\mathbb{R})$, the special group of orthogonal transformations of V. We also proved that $B(q)$ can represent a rotation which will be important to us later in the project.

We will now finish this section with a simple corollary.

Corollary 3.2.16. $O_4(\mathbb{R}) = (L(S^3) \circ R(S^3))\langle\rho\rangle$.

Proof. The map ρ taking q to $-\overline{q}$ is an element of $O_4(\mathbb{R})$ of determinant -1. The group $SO_4(\mathbb{R})$ consists of all elements of $O_4(\mathbb{R})$ of determinant 1. Thus $O_4(\mathbb{R}) = SO_4(\mathbb{R})\langle\rho\rangle$. By Proposition 3.2.15, $L(S^3) \circ R(S^3) = SO_4(\mathbb{R})$, so we have shown that $O_4(\mathbb{R}) = (L(S^3) \circ R(S^3))\langle\rho\rangle$. □

3.3 Unitary Groups

In this section we are going to find out about unitary groups. In this chapter so far we have proved that there is a homomorphism from the unit quaternions to the group of linear transformations, $SL_4(\mathbb{R})$, and extended this to the groups of orthogonal transformations $SO_4(\mathbb{R})$ and $SO_3(\mathbb{R})$. To finish this chapter we are now going to show that there is an isomorphism between S^3 and the unitary group $SU_2(\mathbb{C})$.

To be able to define unitary groups we need to define the Hermitian inner product on $\mathbb{H}$. To be able to do so, we first need to define the Hermitian inner product on a complex vector space.

Definition 3.3.1 (Hermitian Inner Product [6])**.** A *Hermitian inner product* on a complex vector space X is a function that associates a complex number $\langle u, v\rangle$ to each pair of vectors $u, v \in X$ and satisfies the following axioms for all $u, v, w \in X$ and all scalars α:

1. $\langle u + v, w\rangle = \langle u, w\rangle + \langle v, w\rangle$,

2. $\langle u, v + w\rangle = \langle u, v\rangle + \langle u, w\rangle$,

3. $\langle \alpha u, v\rangle = \alpha\langle u, v\rangle$,

4. $\langle u, \alpha v\rangle = \overline{\alpha}\langle u, v\rangle$,

5. $\langle u, v\rangle = \overline{\langle v, u\rangle}$,

6. $\langle u, u\rangle \geq 0$ where $\langle u, u\rangle = 0$ if and only if $u = 0$.

Let us regard the quaternions as a 2-dimensional vector space over $\mathbb{C} = \mathbb{R}[i]$. Then for $q, r \in \mathbb{H}$ write $q\overline{r} = (q, r) + [q, r]j$ where (q, r) and $[q, r]$ belong to $\mathbb{C}$. Then

$$(q, r) = \frac{1}{2}(q\overline{r} - iq\overline{r}i).$$

In the next proposition we see that (q, r) is a Hermitian inner product on $\mathbb{H}$, so part of the proof will be to check if it satisfies the six axioms defined above.

Proposition 3.3.2. *Let $q, r \in \mathbb{H}$. Then (q, r) is the unique Hermitian inner product on $\mathbb{H}$ such that $(q, q) = N(q)$ for all $q \in \mathbb{H}$.*

Proof. To show that (q, r) is a Hermitian inner product on $\mathbb{H}$ we must check the axioms from the definition. Let $q, r, s \in \mathbb{H}$ and let $\alpha \in \mathbb{C}$. Firstly, we check the first axiom,

$(q + r, s) = (q, s) + (r, s)$, as follows:

$$\begin{aligned}(q + r, s) &= \frac{1}{2}((q + r)\overline{s} - i(q + r)\overline{s}i)\\ &= \frac{1}{2}(q\overline{s} + r\overline{s} - iq\overline{s}i - ir\overline{s}i)\\ &= \frac{1}{2}(q\overline{s} - iq\overline{s}i) + \frac{1}{2}(r\overline{s} - ir\overline{s}i)\\ &= (q, s) + (r, s).\end{aligned}$$

Next we will check axiom 5 that $(q, r) = \overline{(r, q)}$ is satisfied:

$$\begin{aligned}\overline{(r, q)} &= \overline{\frac{1}{2}(r\overline{q} - ir\overline{q}i)}\\ &= \frac{1}{2}(\overline{r\overline{q}} - i\overline{r\overline{q}}i)\\ &= \frac{1}{2}(\overline{\overline{q}}\overline{r} - i\overline{\overline{q}}\overline{r}i) && \text{(By Proposition 2.3.5(ii))}\\ &= \frac{1}{2}(q\overline{r} - iq\overline{r}i) && \text{(By Proposition 2.3.5(ii))}\\ &= (q, r).\end{aligned}$$

Now that we know that axioms 1 and 5 are true, we can check axiom 2, $(q, r + s) = (q, r) + (q, s)$, as follows:

$$\begin{aligned}(q, r + s) &= \overline{(r + s, q)} && \text{(By axiom 5)}\\ &= \overline{(r, q) + (s, q)} && \text{(By axiom 1)}\\ &= \overline{(r, q)} + \overline{(s, q)} && \text{(By Proposition 2.3.5(ii))}\\ &= (q, r) + (q, s) && \text{(By axiom 5).}\end{aligned}$$

Next we check the third axiom that $(\alpha q, r) = \alpha(q, r)$:

$$\begin{aligned}(\alpha q, r) &= \frac{1}{2}(\alpha q\overline{r} - i\alpha q\overline{r}i)\\ &= \frac{1}{2}(\alpha q\overline{r} - \alpha iq\overline{r}i) && \text{(By commutativity of } \mathbb{C})\\ &= \alpha(\frac{1}{2}(q\overline{r} - iq\overline{r}i))\\ &= \alpha(q, r).\end{aligned}$$

Now we can show that the fourth axiom $(q, \alpha r) = \overline{\alpha}(q, r)$ is true by using axioms 3 and 5 as follows:

$$\begin{aligned}
(q, \alpha r) &= \overline{(\alpha r, q)} && \text{(By axiom 5)}\\
&= \overline{\alpha}\overline{(r, q)} && \text{(By axiom 3)}\\
&= \overline{\alpha}(q, r) && \text{(By axiom 5).}
\end{aligned}$$

Finally, we prove the sixth axiom that $(q, q) \geq 0$ for all $q \in \mathbb{H}$ where $(q, q) = 0$ if and only if $q = 0$:

$$\begin{aligned}
(q, q) &= \frac{1}{2}(q\overline{q} - iq\overline{q}i)\\
&= \frac{1}{2}(N(q) - iN(q)i)\\
&= \frac{1}{2}(N(q) - N(q)i^2) && \text{(Since the norm is a real number)}\\
&= \frac{1}{2}(N(q) + N(q)) = N(q).
\end{aligned}$$

We have seen previously that $N(q) \geq 0$ for all $q \in \mathbb{H}$ with equality if and only if $q = 0$. Hence we have shown that the sixth axiom of the Hermitian inner product is satisfied as well as the second part of the proposition that $(q, q) = N(q)$ for all $q \in \mathbb{H}$.
Now we have to show that (q, r) is unique (i.e. the only inner product in $\mathbb{H}$ with the property that $(q, q) = N(q)$). Similarly to the proof of Lemma 3.2.5, we can note that

$$\begin{aligned}
N(q + r) &= (q + r, q + r) && \text{(By Lemma 3.2.5)}\\
&= (q, q) + (r, r) + (q, r) + (r, q)\\
&= N(q) + N(r) + (q, r) + (r, q),
\end{aligned}$$

which implies that $(q, r) + (r, q) = N(q + r) - N(q) - N(r)$. Then we also have

$$\begin{aligned}
N(q + ir) &= (q + ir, q + ir) && \text{(By Lemma 3.2.5)}\\
&= (q, q) + i\overline{i}(r, r) + \overline{i}(q, r) + i(r, q)\\
&= (q, q) - i^2(r, r) - i(q, r) + i(r, q) && \text{(Since } \overline{i} = -i\text{)}\\
&= N(q) + N(r) - i(q, r) + i(r, q) && \text{(By axiom 6),}
\end{aligned}$$

which implies that $-i((q, r) - (r, q)) = N(q + ir) - N(q) - N(r)$. Since $\frac{1}{-i} = i$, this is the same as

$$(q, r) - (r, q) = i(N(q + ir) - N(q) - N(r)).$$

We can express (q,r) as $(q,r) = \frac{1}{2}((q,r)+(r,q)+(q,r)-(r,q))$ and since (q,r) can be expressed in terms of $(q,r)+(r,q)$ and $(q,r)-(r,q)$, then (q,r) is uniquely expressed in terms of the norms, $N(q), N(r), N(q+r), N(q+ir)$, as required. □

So we have not only proved that $(q,r) = \frac{1}{2}(q\overline{r} - iq\overline{r}i)$ is a Hermitian inner product on $\mathbb{H}$, but that it has the property that $(q,q) = N(q)$ and is unique with this property. Now we can define unitary groups as follows.

Definition 3.3.3 (Unitary Groups [1])**.** The group of all non-zero $\mathbb{C}$-linear transformations that preserve the Hermitian inner product on a 2-dimensional complex vector space is the *unitary group* $U_2(\mathbb{C})$. The group of transformations in $U_2(\mathbb{C})$ of determinant 1 is the *special unitary group* $SU_2(\mathbb{C})$.

So if we view the quaternions as a 2-dimensional vector space over $\mathbb{C}$, then any $\mathbb{C}$-linear transformation that satisfies the Hermitian inner product (q,r) with $(q,q) = N(q)$ will be in the unitary group $U_2(\mathbb{C})$. To show that a $\mathbb{C}$-linear transformation is in $SU_2(\mathbb{C})$ we also need to show that it has determinant 1. In the following proposition, we see that there is an easy way of calculating the determinant of the linear transformation $R(q)$.

Proposition 3.3.4. *Given $q = \alpha + \beta j$ where $\alpha, \beta \in \mathbb{C}$, the matrix of $R(q)$, considered as a $\mathbb{C}$-linear transformation of the space $\mathbb{H}$ with respect to the basis $\{1, j\}$ is*

$$R(q) = \begin{pmatrix} \overline{\alpha} & \overline{\beta} \\ -\beta & \alpha \end{pmatrix},$$

with determinant $N(q)$ and trace $Tr(q)$.

Proof. The matrix of $R(q)$ with respect to the basis is computed by applying the map $R(q)$ explicitly to the basis elements $1, j$. Firstly we get

$$R(q)1 = \overline{q} = \overline{\alpha}(1) - \beta(j)$$

by Proposition 2.3.5(i). Now note that we can write $\alpha = a + bi$ and $\beta = c + di$ where

$a, b, c, d \in \mathbb{R}$. Using this we get

$$\begin{aligned}
R(q)j = j\overline{q} &= j(\overline{\alpha}1 - \beta j) \\
&= j\overline{\alpha} - j\beta j \\
&= j(a - bi) - j(c + di)j \\
&= (aj - bji) - (cj^2 + djij) \\
&= (aj + bij) - (cj^2 - dij^2) && \text{(Since } ij = -ji\text{)} \\
&= (a + bi)j - (c - di)j^2 \\
&= \alpha j - \overline{\beta}j^2 \\
&= \overline{\beta}(1) + \alpha(j).
\end{aligned}$$

By letting each computation of $R(q)$ be represented by columns of the matrix with rows representing the coefficients $1, j$ we get

$$R(q) = \begin{pmatrix} \overline{\alpha} & \overline{\beta} \\ -\beta & \alpha \end{pmatrix}$$

as required. The determinant of this matrix is given by $\alpha\overline{\alpha} - \beta\overline{\beta} = N(q)$ by Proposition 2.3.5(i). The trace of the matrix is given by $\alpha + \overline{\alpha} = Tr(q)$ by Proposition 2.3.5(i). $\square$

Since the determinant of $R(q)$ is equal to the norm $N(q)$, then it is clear that $\det R(q) = N(q) = 1$ if $q \in S^3$. Therefore, for $q \in S^3$, we have that $R(q) \in SU_2(\mathbb{C})$ if $R(q)$ preserves the Hermitian inner product $(q, r) = \frac{1}{2}(q\overline{r} - iq\overline{r}i)$ and we prove that this is the case in the following lemma.

Lemma 3.3.5. *$R(q) \in SU_2(\mathbb{C})$ for all $q \in S^3$.*

Proof. To show that $R(q) \in U_2(\mathbb{C})$ we need to show that it preserves the Hermitian inner product. To do so we check that $(R(q)u, R(q)v) = (u, v)$ for all $u, v \in \mathbb{H}$. We show this as follows:

$$
\begin{aligned}
(R(q)u, R(q)v) &= (u\overline{q}, v\overline{q}) \\
&= \frac{1}{2}(u\overline{q}\,\overline{v\overline{q}} - iu\overline{q}\,\overline{v\overline{q}}i) && \text{(By definition)} \\
&= \frac{1}{2}(u\overline{q}\,\overline{\overline{q}}\,\overline{v} - iu\overline{q}\,\overline{\overline{q}}\,\overline{v}i) && \text{(By Proposition 2.3.5(ii))} \\
&= \frac{1}{2}(u\overline{q}q\overline{v} - iu\overline{q}q\overline{v}i) && \text{(By Proposition 2.3.5(ii))} \\
&= \frac{1}{2}(uN(\overline{q})\overline{v} - iuN(\overline{q})\overline{v}i) && \text{(By definition)} \\
&= \frac{1}{2}(u\overline{v} - iu\overline{v}i) && \text{(Since } N(\overline{q}) = N(q) = 1 \text{ for all } q \in S^3\text{)} \\
&= (u, v)
\end{aligned}
$$

as required. Then it is clear that $R(q) \in SU_2(\mathbb{C})$ since by Proposition 3.3.4 we have that the determinant of the matrix of $R(q)$ is the norm of q and we know that $N(q) = 1$ for all $q \in S^3$. □

Now that we know that $R(q)$ maps elements in S^3 to $SU_2(\mathbb{C})$, it follows that there is a homomorphism from S^3 to $SU_2(\mathbb{C})$ as we have already proved earlier in this chapter that $R(q)$ is a homomorphism when $q \in S^3$. It turns out that the map $R(q)$ from S^3 to $SU_2(\mathbb{C})$ is an isomorphism so in this next proposition we will prove that the map is bijective.

Proposition 3.3.6. *The map $R\colon S^3 \to SU_2(\mathbb{C})$ is an isomorphism.*

Proof. We know that $R(q) \in SU_2(\mathbb{C})$ for all $q \in S^3$ by Lemma 3.3.5. Alcock-Zeilinger [7] tells us that we can write $SU_2(\mathbb{C})$ as

$$\left\{ \begin{pmatrix} \overline{\alpha} & \overline{\beta} \\ -\beta & \alpha \end{pmatrix} : |\alpha|^2 + |\beta|^2 = 1 \right\}$$

since the determinant of transformations in $SU_2(\mathbb{C})$ are equal to 1. We already know that $R(q)$ is a homomorphism when $q \in S^3$ by Lemma 3.1.10. Now we need to show that $R : S^3 \to SU_2(\mathbb{C})$ is injective and surjective.

To show that the function is injective we need to show that the kernel is just the identity. Thus the kernel is given by

$$\ker R = \left\{ q = \alpha + \beta j : |\alpha|^2 = |\beta|^2 = 1, \begin{pmatrix} \overline{\alpha} & \overline{\beta} \\ -\beta & \alpha \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \right\}.$$

Clearly, $q = 1 + 0j = 1$ is the only possible element of $\ker R$ which shows that R is injective.

Finally, R is surjective because every matrix

$$\begin{pmatrix} \overline{\alpha} & \overline{\beta} \\ -\beta & \alpha \end{pmatrix} \in SU_2(\mathbb{C})$$

is in the image of R (i.e. is $R(\alpha + \beta j)$). $\square$

So we have shown that S^3 and $SU_2(\mathbb{C})$ are isomorphic. Therefore it is clear that $SU_2(\mathbb{C})$ is a subgroup of the group of non-zero quaternions.

The unit circle in $\mathbb{C}$ is $S^1 := \{\alpha \in \mathbb{C} \mid N(\alpha) = 1\}$ and if $\alpha \in S^1$, the map $L(\alpha)$ is $\mathbb{C}$-linear and preserves the Hermitian inner product. We will finish this section with the following proposition showing that there is a homomorphism from the Cartesian product $S^1 \times S^3$ onto $U_2(\mathbb{C})$.

Proposition 3.3.7. *The map* $S^1 \times S^3 \to U_2(\mathbb{C})\colon (\alpha, q) \mapsto L(\alpha)R(q)$ *is a homomorphism onto* $U_2(\mathbb{C})$ *with kernel* $\{(1,1), (-1,-1)\}$.

Proof. To show that $S^1 \times S^3 \to U_2(\mathbb{C})$ is a homomorphism we must check that $L(\alpha_1\alpha_2)R(q_1q_2) = L(\alpha_1)R(q_1)L(\alpha_2)R(q_2)$ for $\alpha_1, \alpha_2 \in \mathbb{C}$ and $q_1, q_2 \in S^3$. We already know that L and R are homomorphisms in S^3 and $L(\alpha)$ commutes with $R(q)$, so

$$\begin{aligned} L(\alpha_1\alpha_2)R(q_1q_2) &= L(\alpha_1)L(\alpha_2)R(q_1)R(q_2) \\ &= L(\alpha_1)R(q_1)L(\alpha_2)R(q_2). \end{aligned}$$

We then must show that the kernel is $\{(1,1), (-1,-1)\}$ and that it is surjective.

By Proposition 3.2.15, the only elements sent to the identity by $L(r)R(q)$ for $q, r \in \mathbb{H}$ are $(1,1)$ and $(-1,-1)$ so $\ker L(\alpha)R(q) = \{(1,1), (-1,-1)\}$ since both of these pairs are in $S^1 \times S^3$.

We have that $\{R(q) \mid q \in S^3\} = SU_2(\mathbb{C})$ by Proposition 3.3.6. To show that the map $S^1 \times S^3 \to U_2(\mathbb{C})$ is surjective, we need to write an arbitrary element $X \in U_2(\mathbb{C})$ in the form αM where $\alpha \in \mathbb{C}, |\alpha| = 1$, and $M \in SU_2(\mathbb{C})$. Let $\beta = \det X$ and take $\alpha \in \mathbb{C}$

such that $\alpha^2 = \beta$. Then put $M = \alpha^{-1}X$ so that $X = \alpha M$. Then we have

$$\begin{aligned}\beta = \det X = \det&\left(\begin{pmatrix}\alpha & 0\\ 0 & \alpha\end{pmatrix} M\right)\\ = \det&\begin{pmatrix}\alpha & 0\\ 0 & \alpha\end{pmatrix}\det M\\ =\ &\alpha^2 \det M = \beta \det M.\end{aligned}$$

Since X is invertible, we have $\beta \neq 0$. Hence $\det M$ must be 1. Then we have

$$\begin{aligned}M\overline{M^T} &= \alpha^{-1}\overline{\alpha^{-1}}X\overline{X^T}\\ &= |\alpha^{-1}|^2 X\overline{X^T}\\ &= |\beta^{-1}|X\overline{X^T}.\end{aligned}$$

But $X\overline{X^T} = I_2$, the 2×2 identity matrix, and $|\beta|^2 = 1$. We have $\det X \det \overline{X^T} = \det X \overline{\det X} = |\det X|^2$, so $|\det X|^2 = \det I_2 = 1$ implying that $\det X = 1$. Therefore $X \in SU_2(\mathbb{C})$ and hence we have a surjective map. $\square$

To conclude, the main things to take away from this chapter are the following.

- The definition of the unit quaternions, S^3, and the fact that S^3 is a subgroup of the group of non-zero quaternions, $\mathbb{H}\backslash\{0\}$.
- The definition of the group of linear transformations of $\mathbb{H}$, $SL_4(\mathbb{R})$, and the monomorphism from S^3 to $SL_4(\mathbb{R})$.
- The definition of pure quaternions.
- The definitions of orthogonal groups $SO_4(\mathbb{R})$ and $SO_3(\mathbb{R})$ and the homomorphisms from S^3 to $SO_4(\mathbb{R})$ and $SO_3(\mathbb{R})$.
- The fact that the linear transformation $B(q)$ can represent a rotation through an angle θ with $q = \cos\frac{1}{2}\theta + u\sin\frac{1}{2}\theta$ where u is a pure quaternion with norm 1.
- The definition of the unitary group $SU_2(\mathbb{C})$ and the isomorphism from S^3 to $SU_2(\mathbb{C})$.

The things that we have learned in this chapter will lead to some of the results that will come up in the next chapter.

Chapter 4

The Finite Subgroups of Quaternions

If $q \in \mathbb{H}\backslash\{0\}$ has finite order, then it follows from Proposition 2.3.5(iii) that $N(q) = 1$. Thus every finite subgroup of $\mathbb{H}\backslash\{0\}$ is a subgroup of S^3. The only element of order 2 in S^3 is -1 so one might expect the possible types of finite subgroups to be quite limited. Under the homomorphism $B\colon S^3 \to SO_3(\mathbb{R})$ of Proposition 3.2.10, the groups in question are the inverse images of cyclic groups, dihedral groups, and the rotation groups of the Platonic solids. In this chapter, we show that these finite groups are subgroups of $\mathbb{H}\backslash\{0\}$, but we do not show the fact that every finite subgroup of $\mathbb{H}\backslash\{0\}$ is conjugate to one of these.

4.1 Cyclic Groups and Dihedral Groups

We will begin the chapter by defining cyclic groups and dihedral groups.

Definition 4.1.1 (Cyclic Group [3])**.** A *cyclic group* is a group that is generated by a single element x, the *group generator*. A cyclic group of finite order n is denoted $\mathcal{C}_n$ and its generator x satisfies $x^n = I$ where I is the identity element. Cyclic groups are abelian.

Example 4.1.2. (1) The finite cyclic groups $\mathcal{C}_n$ can be described as the groups of rotations of a regular n-gon where $n \in \mathbb{Z}_{>0}$. For example $\mathcal{C}_3$ is the group of rotations of an equilateral triangle.

(2) The additive group of integers $\mathbb{Z}$ is the infinite cyclic group. Every cyclic group is isomorphic to either $\mathcal{C}_n$ or $\mathbb{Z}$.

(3) $\mathcal{C}_n$ is isomorphic to $\mathbb{Z}_n$ (the group of integers modulo n). We usually write $\mathcal{C}_n$ multiplicatively while we write $\mathbb{Z}_n$ additively.

In example 4.1.2 (1) we see that the finite cyclic groups $\mathcal{C}_n$ can be described as the groups of rotations of a regular n-gon. We have also seen in the previous chapter that the map $B(q)$ can also represent rotations of regular n-gons when q is a unit quaternion. This shows that $\mathcal{C}_n$ is a subgroup of the unit quaternions. Therefore $\mathcal{C}_n$ is a finite subgroup of $\mathbb{H}\backslash\{0\}$.

Definition 4.1.3 (Dihedral Group [3])**.** The *dihedral group* is the symmetry group of a regular n-gon where $n \geq 2$. The dihedral group of order $2n$ is denoted D_n.

Remark Symmetry groups of regular n-gons with $n \geq 3$ are isomorphic to non-abelian permutation groups. Therefore we can also interpret dihedral groups as permutation groups as we see in the following example.

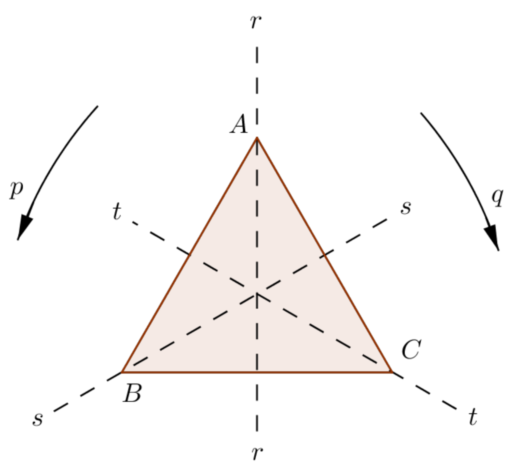

Figure 4.1: Dihedral Group D_3 [8].

Example 4.1.4. The dihedral group D_3 is the symmetry group of the equilateral triangle. Let ABC denote an equilateral triangle (Figure 4.1). Then the following are symmetry mappings on ABC.

- $e = (A)(B)(C)$ is the identity map.
- $p = R_{\frac{2\pi}{3}} = (ABC)$ is the anti-clockwise rotation of 120° about the centre.
- $q = R_{-\frac{2\pi}{3}} = (ACB)$ is the clockwise rotation of 120° about the centre.
- $r = S_r = (BC)$ is the reflection in the line r (Figure 4.1).
- $s = S_s = (AC)$ is the reflection in the line s (Figure 4.1).
- $t = S_t = (AB)$ is the reflection in the line t (Figure 4.1).

These six operations form the group D_3.

Dihedral groups are not finite subgroups of the non-zero quaternions. However, the following definition gives us a specific type of dihedral groups that are finite subgroups of $\mathbb{H}\backslash\{0\}$.

Definition 4.1.5 (Binary Dihedral Group [1])**.** For every integer $n \geq 2$, the *binary dihedral group* (or *dicyclic group*), $\mathcal{D}_{2n}$, can be defined as the subgroup of the unit quaternions, S^3, generated by $a = e^{\frac{i\pi}{n}} = \cos\frac{\pi}{n} + i\sin\frac{\pi}{n}$ and $x = j$. Equivalently, we can define $\mathcal{D}_{2n}$ as the group with presentation

$$\mathcal{D}_{2n} = \langle a, x \mid a^{2n} = 1, x^2 = a^n, x^{-1}ax = a^{-1}\rangle.$$

Proposition 4.1.6. *The following results come directly from the definition:*

(i) $x^4 = 1$,

(ii) $x^2a^m = a^{m+n} = a^mx^2$,

(iii) $a^mx^{-1} = a^{m-n}x$.

Proof. We can explicitly show the results above from the definition of a binary dihedral group.

(i) $x^4 = j^4 = (j^2)^2 = (-1)^2 = 1$.

(ii) $x^2a^m = a^na^m = a^{n+m} = a^{m+n} = a^ma^n = a^mx^2$.

(iii) $a^mx^{-1} = a^{m-n}a^nx^{-1} = a^{m-n}x^2x^{-1} = a^{m-n}x$.

□

Thus every element of $\mathcal{D}_{2n}$ can be uniquely written as $a^m x^l$ where $0 \leq m \leq 2n$ and $l = 0$ or $l = 1$. The multiplication rules are given by:

- $a^k a^m = a^{k+m}$,
- $a^k a^m x = a^{k+m} x$,
- $a^k x a^m x = a^{k-m+n}$.

Proposition 4.1.7. *The binary dihedral group $\mathcal{D}_{2n}$ is an extension of $\mathcal{C}_2$ (the cyclic group of order 2) by $\mathcal{C}_{2n}$ (the cyclic group of order $2n$). This extension can be expressed by*

$$\mathcal{C}_{2n} \xrightarrow{\phi} \mathcal{D}_{2n} \xrightarrow{\psi} \mathcal{C}_2$$

where $\phi : \mathcal{C}_{2n} \to \mathcal{D}_{2n}$ is injective, $\psi : \mathcal{D}_{2n} \to \mathcal{C}_2$ is surjective, and $\ker \psi = \operatorname{im} \phi$.

Proof. The cyclic group $\mathcal{C}_{2n}$ consists of the elements $\{1, c, c^2, \ldots, c^{2n-1}\}$ where c generates the group. We can define a map $\phi : \mathcal{C}_{2n} \to \mathcal{D}_{2n}$ such that $c^k \mapsto a^k$ where $c \in \mathcal{C}_{2n}$, $a \in \mathcal{D}_{2n}$, and $k \in \mathbb{N}$. Then we see that this is a homomorphism because

$$\begin{aligned} \phi(c^k c^l) &= \phi(c^{k+l}) \\ &= a^{k+l} = a^k a^l = \phi(c^k)\phi(c^l). \end{aligned}$$

Now consider the cyclic group $\mathcal{C}_2 = \{-1, 1\}$. We can define a map $\psi : \mathcal{D}_{2n} \to \mathcal{C}_2$ such that $a \mapsto 1$ and $x \mapsto -1$ where $a, x \in \mathcal{D}_{2n}$. To check that ψ is a homomorphism we can look at the relations of $\mathcal{D}_{2n} = \langle a, x \mid a^{2n} = 1, x^2 = a^n, x^{-1}ax = a^{-1} \rangle$ and check that ψ satisfies these relations. We have

$$\psi(a)^{2n} = 1^{2n} = 1$$

as required. We also have

$$\psi(x)^2 = (-1)^2 = 1 = 1^2 = \psi(a)^2$$

as required. Finally, we have

$$\psi(x)^{-1}\psi(a)\psi(x) = (-1)^{-1}(1)(-1) = 1 = 1^{-1} = \psi(a)^{-1}$$

as required, and hence ψ is a homomorphism.
As $\psi(a^k x^l) = 1^k(-1)^l = (-1)^l$, we have that

$$\ker \psi = \{a^k x^l \mid l = 0\} = \{a^k\} = \operatorname{im} \phi$$

and this is also enough to show that ϕ is injective and ψ is surjective. $\square$

Remark Note that $x^2 = a^n \in \mathcal{D}_{2n}$ is an element of order 2 (since $(x^2)^2 = (a^n)^2 = a^{2n} = 1$) and the centre of $\mathcal{D}_{2n}$ consists solely of the identity element and x^2. If we add the relation $x^2 = 1$ to the presentation of $\mathcal{D}_{2n}$ we would obtain the presentation of the dihedral group, D_n. This means that the quotient group $\mathcal{D}_{2n}/\langle x^2\rangle \cong D_n$.

Just like dihedral groups, binary dihedral groups are non-abelian. However, they have order $4n$ rather than $2n$. We also have from Lehrer and Taylor [1] that the binary dihedral group $\mathcal{D}_{2n}$ where $n = 2$ is isomorphic to the *quaternion group* $\mathcal{Q} = \{\pm 1, \pm i, \pm j, \pm k\}$. The quaternion group, $\mathcal{Q}$, is a subgroup of $\mathbb{H}\backslash\{0\}$, meaning that by isomorphism the binary dihedral group is too. Now we will see another way of showing that the binary dihedral group is a subgroup of $\mathbb{H}\backslash\{0\}$ in the following proposition.

Proposition 4.1.8. *The binary dihedral group, $\mathcal{D}_{2n}$, is a subgroup of $\mathbb{H}\backslash\{0\}$.*

Proof. Firstly we will construct a subgroup of $\mathbb{H}\backslash\{0\}$ as follows. For each positive integer m, let $\zeta_m := \exp\frac{2\pi i}{m} = \cos\frac{2\pi}{m} + i\sin\frac{2\pi}{m}$. Let $\mathbf{C}_m$ denote the cyclic subgroup of $\mathbb{H}\backslash\{0\}$ of order m generated by ζ_m and let $\mathbf{D}_m$ denote the subgroup of $\mathbb{H}\backslash\{0\}$ generated by ζ_m and j. For $\alpha \in \mathbf{C}_m$ we have $j\alpha j^{-1} = \overline{\alpha} = \alpha^{-1}$ so $\mathbf{C}_m$ is a normal subgroup of $\mathbf{D}_m$ ($\mathbf{C}_m \trianglelefteq \mathbf{D}_m$).

It follows that if m is even ($m = 2n$), then $\mathbf{D}_m = \mathcal{D}_{2n}$ is the binary dihedral group. Now let m be odd. Note that $j \in \mathbf{D}_m$ and $j^2 = -1 = e^{-\pi i}$. Also, note that

$$\begin{aligned}\frac{2\pi i}{2m} &= \frac{2\pi i}{2m} + \frac{2m\pi i}{2m} - \frac{2m\pi i}{2m} \\ &= \frac{2\pi i}{m}\left(\frac{m+1}{2}\right) - \pi i.\end{aligned}$$

Then we can rearrange $\zeta_{2m} \in \mathbf{D}_{2m}$ as follows:

$$\begin{aligned}\zeta_{2m} &= \exp\left(\frac{2\pi i}{2m}\right) \\ &= \exp\left(\frac{2\pi i}{m}\right)^{\frac{m+1}{2}} \exp(-\pi i) \\ &= \zeta_m^{\frac{m+1}{2}} j^2 && \text{(Since } j^2 = e^{-\pi i}).\end{aligned}$$

Since m is odd, $\frac{m+1}{2}$ is an integer which means that $\zeta_m^{\frac{m+1}{2}} j^2 \in \mathbf{D}_m$, so $\mathbf{D}_{2m} \subseteq \mathbf{D}_m$. Also, if m is odd, then we have $\zeta_m = \zeta_{2m}^2 \in \mathbf{D}_{2m}$. Clearly $j \in \mathbf{D}_{2m}$ since it generates $\mathbf{D}_m$, so we have $\mathbf{D}_m \subseteq \mathbf{D}_{2m}$. Therefore, if m is odd, $\mathbf{D}_m = \mathbf{D}_{2m}$.

If m is odd, then $2m$ is even. We have already seen that $\mathbf{D}_m = \mathcal{D}_{2n}$ when m is even. Thus, when m is odd, we have $\mathbf{D}_m = \mathbf{D}_{2m} = \mathcal{D}_{2n}$. Therefore $\mathbf{D}_m = \mathcal{D}_{2n}$ for all positive integers m. Hence, since $\mathbf{D}_m$ is a subgroup of $\mathbb{H}\backslash\{0\}$ then so is $\mathcal{D}_{2n}$, as required. $\square$

4.2 Polyhedral Groups and Final Theorem

From Proposition 3.1.12, two elements of S^3 are conjugate if and only if they have the same trace. For the following definitions of polyhedral groups, we are going to need to know the trace of certain small order elements of S^3 given in the following table from Lehrer and Taylor [1].

Trace Table

order	3	4	5	6	8	10
trace	-1	0	$-\tau, \tau^{-1}$	1	$\pm\sqrt{2}$	$\tau, -\tau^{-1}$

where $\tau = \frac{1}{2}(1+\sqrt{5})$.

Example 4.2.1 (Verify the entries of the trace table)**.** Recall that if we let $q = \cos\frac{1}{2}\theta + u\sin\frac{1}{2}\theta$ for some $u \in V$ such that $N(u) = 1$, then $B(q)$ is a rotation of angle θ about axis u. The entries of the trace table are then given by the trace of q for different values of θ. Note that the trace is given by $Tr(q) = 2a$ where $q = a + bi + cj + dk$ (with $a, b, c, d \in \mathbb{R}$). Hence, $Tr(q) = 2a = 2\cos\frac{1}{2}\theta$. Since $u \in V$, it can be given by $u = bi + cj + dk$, and we have $N(u) = b^2 + c^2 + d^2$. So for this example, we can choose $u = i + (0j + 0k)$ so that we get $N(u) = 1^2 + 0^2 + 0^2 = 1$.

<u>Order 3:</u> Consider a quaternion representing a $120°$ rotation ($\theta = \frac{2\pi}{3}$) around the axis $u = i$. This rotation has order 3 and can be represented by $B(q)$ so we need to check if q also has order 3. We get

$$\begin{aligned} q &= \cos\frac{1}{2}\theta + u\sin\frac{1}{2}\theta \\ &= \cos\frac{\pi}{3} + i\sin\frac{\pi}{3} = \frac{1}{2} + \frac{\sqrt{3}}{2}i. \end{aligned}$$

However, here we have $q^3 = -1$ which means that the order is 6. To try and solve this problem, we have that $B(-q)$ can also represent a rotation of order 3

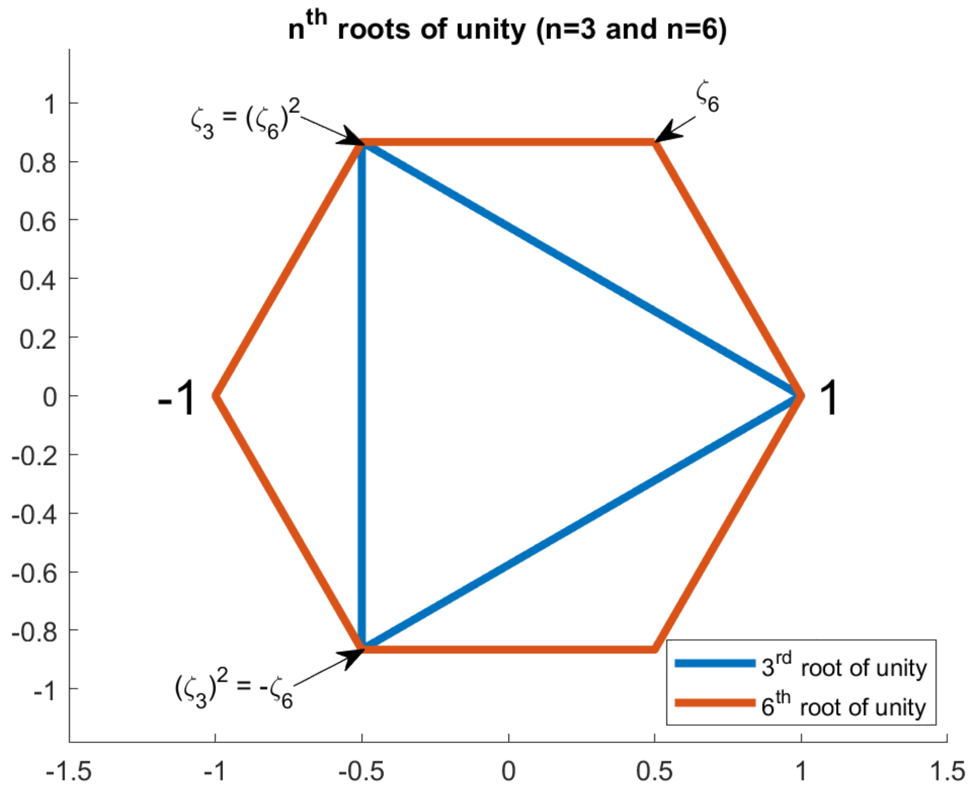

Figure 4.2: A graph of the n^{th} roots of unity for $n = 3$ and $n = 6$ (i.e. ζ_3 and ζ_6). (Graph created using Matlab [9]).

since $B(q) = B(-q)$. Hence we can also check if $-q$ has order 3. We have

$$-q = -\cos\frac{\pi}{3} - i\sin\frac{\pi}{3} = -\frac{1}{2} - \frac{\sqrt{3}}{2}i,$$

and this time we have that $(-q)^3 = 1$, so $-q$ has order 3. So now we check the norm of $-q$ is 1 and we get

$$N(q) = (-q)(\overline{-q}) = \left(-\frac{1}{2} - \frac{\sqrt{3}}{2}i\right)\left(-\frac{1}{2} + \frac{\sqrt{3}}{2}i\right) = \frac{1}{4} + \frac{3}{4} = 1$$

as required. Thus we get the following trace:

$$Tr(-q) = 2\left(-\cos\frac{\pi}{3}\right) = 2\left(-\frac{1}{2}\right) = -1,$$

as required. So we have shown that all order 3 elements of S^3 have trace -1.

<u>Order 4:</u> Consider a quaternion representing a 90° rotation ($\theta = \frac{\pi}{2}$) around the axis $u = i$. This rotation has order 4 and can be represented by $B(q)$ so we need

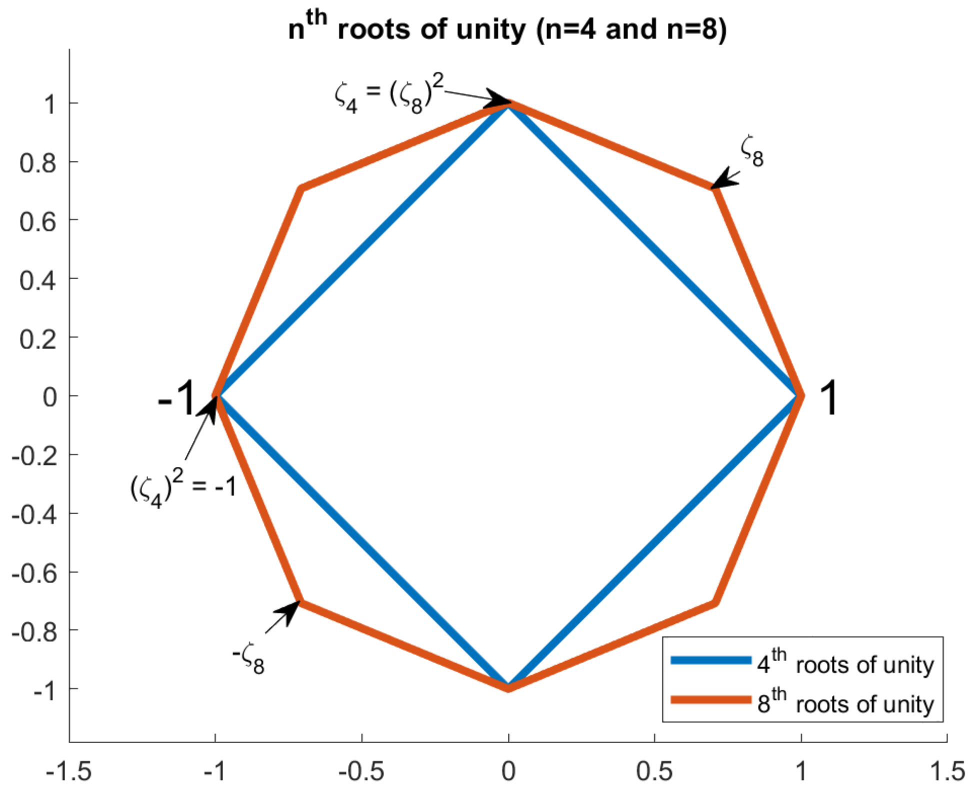

Figure 4.3: A graph of the n^{th} roots of unity for $n = 4$ and $n = 8$ (i.e. ζ_4 and ζ_8). (Graph created using Matlab [9]).

to check if q also has order 4. We get

$$\begin{aligned} q &= \cos\frac{1}{2}\theta + u\sin\frac{1}{2}\theta \\ &= \cos\frac{\pi}{4} + i\sin\frac{\pi}{4} = \frac{\sqrt{2}}{2} + \frac{\sqrt{2}}{2}i. \end{aligned}$$

However, here we have $q^4 = -1$ which means that q has order 8 when $B(q)$ has order 4. To try and solve this problem, we have that $B(-q)$ can also represent a rotation of order 4, so we also check if $-q$ has order 4. We have

$$-q = -\cos\frac{\pi}{4} - i\sin\frac{\pi}{4} = -\frac{\sqrt{2}}{2} - \frac{\sqrt{2}}{2}i$$

but this time we also have $(-q)^4 = -1$ meaning that both q and $-q$ have order 8. Therefore we need to try something different again. In this case, we can try and find the order of q^2 as $B(q^2)$ also represents a rotation of order 4. We get

$$\begin{aligned} q^2 &= \left(\cos\frac{\pi}{4} + i\sin\frac{\pi}{4}\right)^2 \\ &= \left(\frac{\sqrt{2}}{2} + \frac{\sqrt{2}}{2}i\right)\left(\frac{\sqrt{2}}{2} + \frac{\sqrt{2}}{2}i\right) \\ &= \frac{1}{2} + i + \frac{1}{2}i^2 = i \end{aligned}$$

and this time we have $(q^2)^4 = 1$ meaning q^2 has order 4. So now we check the norm is 1 and we get $N(q^2) = q^2\overline{q^2} = (0+i)(0-i) = (-i)^2 = 1$ as required. Thus we get the following trace:

$$Tr(q^2) = 2(0) = 0,$$

as required. So we have shown that all order 4 elements of S^3 have trace 0.

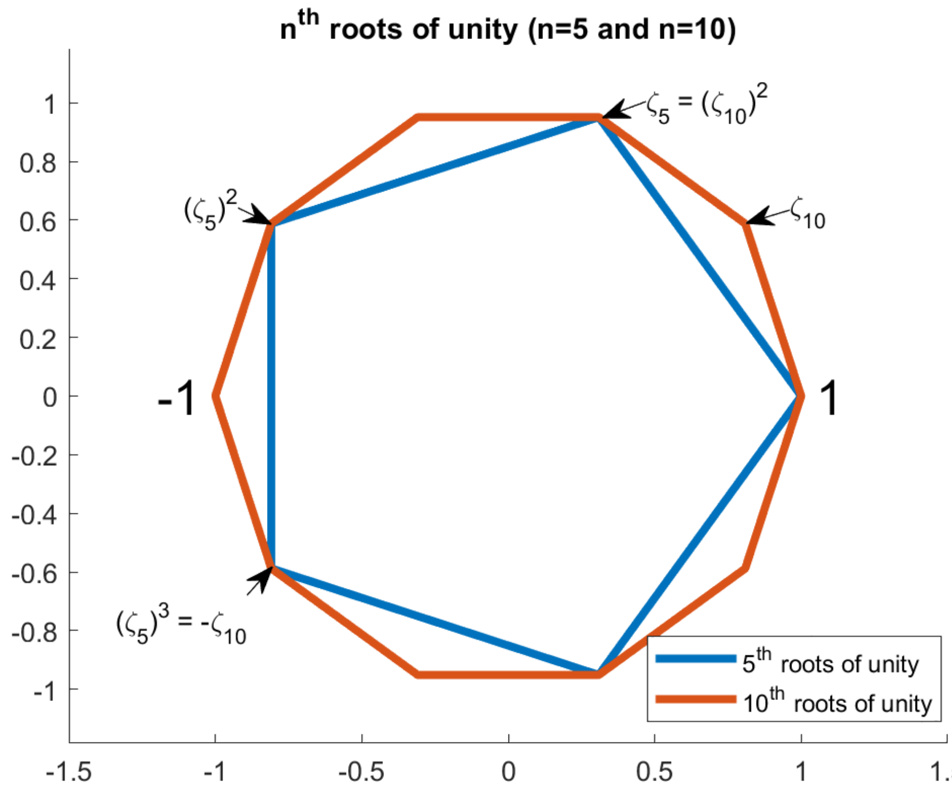

Figure 4.4: A graph of the n^{th} roots of unity for $n = 5$ and $n = 10$ (i.e. ζ_5 and ζ_{10}). (Graph created using Matlab [9]).

Order 5: Consider a quaternion representing a $72°$ rotation ($\theta = \frac{2\pi}{5}$) around the axis $u = i$. This rotation has order 5 and can be represented by $B(q)$ so we need to check if q also has order 5. We get

$$\begin{aligned}q &= \cos\frac{1}{2}\theta + u\sin\frac{1}{2}\theta \\ &= \cos\frac{\pi}{5} + i\sin\frac{\pi}{5} = \frac{1+\sqrt{5}}{4} + \left(\sqrt{\frac{5}{8} - \frac{\sqrt{5}}{8}}\right) i.\end{aligned}$$

However, here we have $q^5 = -1$ which means that q has order 10. Similarly to the above, we check if $-q$ has order 5. We have

$$-q = -\cos\frac{\pi}{5} - i\sin\frac{\pi}{5} = \frac{-1-\sqrt{5}}{4} - \left(\sqrt{\frac{5}{8} - \frac{\sqrt{5}}{8}}\right) i$$

and this time $(-q)^5 = 1$ so $-q$ has order 5. So we check the norm and get

$$\begin{aligned}N(-q) &= (-q)(\overline{-q}) \\ &= \left(\frac{-1-\sqrt{5}}{4} - \left(\sqrt{\frac{5}{8} - \frac{\sqrt{5}}{8}}\right) i\right)\left(\frac{-1-\sqrt{5}}{4} + \left(\sqrt{\frac{5}{8} - \frac{\sqrt{5}}{8}}\right) i\right) \\ &= \left(\frac{-1-\sqrt{5}}{4}\right)^2 - \left(\frac{5}{8} - \frac{\sqrt{5}}{8}\right) i^2 \\ &= \frac{3+\sqrt{5}}{8} + \frac{5}{8} - \frac{\sqrt{5}}{8} \\ &= 1\end{aligned}$$

as required. Then we get the following trace:

$$Tr(-q) = 2\left(-\cos\frac{\pi}{5}\right) = 2\left(\frac{-1-\sqrt{5}}{4}\right) = -\frac{1}{2}(1+\sqrt{5}) = -\tau$$

as required. However, we still need to show that $\tau^{-1} = \frac{-1+\sqrt{5}}{2}$ is also the trace of some order 5 elements of S^3. Consider $B(q^2)$ as a rotation of order 5 and check if q^2 is of order 5. We get

$$\begin{aligned}q^2 &= \left(\cos\frac{\pi}{5} + i\sin\frac{\pi}{5}\right)^2 \\ &= \left(\frac{1+\sqrt{5}}{4} + \left(\sqrt{\frac{5}{8} - \frac{\sqrt{5}}{8}}\right) i\right)^2 \\ &= \frac{3+\sqrt{5}}{8} + \left(\frac{5}{8} - \frac{\sqrt{5}}{8}\right) i^2 + 2i\left(\frac{1+\sqrt{5}}{4}\sqrt{\frac{5}{8} - \frac{\sqrt{5}}{8}}\right) \\ &= \frac{-1+\sqrt{5}}{4} + \frac{1+\sqrt{5}}{2}\left(\sqrt{\frac{5}{8} - \frac{\sqrt{5}}{8}}\right) i\end{aligned}$$

which has order 5 since $(q^2)^5 = 1$. Let $x = \frac{1+\sqrt{5}}{2}\left(\sqrt{\frac{5}{8} - \frac{\sqrt{5}}{8}}\right) i$. Then we have that

$$\begin{aligned}
N(q^2) &= q^2\overline{q^2} \\
&= \left(\frac{-1+\sqrt{5}}{4} + x\right)\left(\frac{-1+\sqrt{5}}{4} - x\right) \\
&= \left(\frac{-1+\sqrt{5}}{4}\right)^2 - x^2 \\
&= \frac{3-\sqrt{5}}{8} + \frac{5}{8} + \frac{\sqrt{5}}{8} \\
&= 1
\end{aligned}$$

as required. Thus we get the following trace:

$$Tr(q^2) = 2\left(\frac{-1+\sqrt{5}}{4}\right) = \frac{-1+\sqrt{5}}{2} = \tau^{-1}$$

as required. So we have shown that order 5 elements of S^3 have trace $-\tau$ or τ^{-1} where $\tau = \frac{1}{2}(1+\sqrt{5})$.

<u>Order 6:</u> Consider a quaternion representing a 60° rotation ($\theta = \frac{\pi}{3}$) around the axis $u = i$. This rotation has order 6 and can be represented by $B(q)$ where

$$\begin{aligned}
q &= \cos\frac{1}{2}\theta + u\sin\frac{1}{2}\theta \\
&= \cos\frac{\pi}{6} + i\sin\frac{\pi}{6} = \frac{\sqrt{3}}{2} + \frac{1}{2}i.
\end{aligned}$$

However, here we have $q^6 = -1$ which means that q has order 12. So to try and solve this problem we check $-q$ has order 6. We have

$$-q = -\cos\frac{\pi}{6} - i\sin\frac{\pi}{6} = -\frac{\sqrt{3}}{2} - \frac{1}{2}i$$

but we still have $(-q)^6 = -1$. Now we check the rotation $B(q^2)$ so we calculate

$$q^2 = \left(\cos\frac{\pi}{6} + i\sin\frac{\pi}{6}\right)^2 = \frac{1}{2} + \frac{\sqrt{3}}{2}i$$

and we see that we have $(q^2)^6 = 1$ meaning that q^2 has order 6. So here we have that

$$N(q^2) = q^2\overline{q^2} = \left(\frac{1}{2} + \frac{\sqrt{3}}{2}i\right)\left(\frac{1}{2} - \frac{\sqrt{3}}{2}i\right) = \frac{1}{4} + \frac{3}{4} = 1$$

as required. Thus we get the following trace:

$$Tr(q) = 2\left(\frac{1}{2}\right) = 1$$

as required. So we have shown that all order 6 elements of S^3 have trace 1.

<u>Order 8:</u> Consider a quaternion representing a 45° rotation ($\theta = \frac{\pi}{4}$) around the axis $u = i$. This rotation has order 8 and can be represented by $B(q)$ where

$$\begin{aligned} q &= \cos\frac{1}{2}\theta + u\sin\frac{1}{2}\theta \\ &= \cos\frac{\pi}{8} + i\sin\frac{\pi}{8} = \frac{\sqrt{2+\sqrt{2}}}{2} + \frac{\sqrt{2-\sqrt{2}}}{2}i. \end{aligned}$$

However, here we have $q^8 = -1$ which means that q has order 16. So to try and solve this problem we check if $-q$ has order 8. We have

$$-q = -\cos\frac{\pi}{8} - i\sin\frac{\pi}{8} = -\frac{\sqrt{2+\sqrt{2}}}{2} - \frac{\sqrt{2-\sqrt{2}}}{2}i$$

but we still have $(-q)^8 = -1$. Now we try the rotation $B(q^2)$ and check that q^2 has order 8. We have

$$\begin{aligned} q^2 &= \left(\cos\frac{\pi}{8} + i\sin\frac{\pi}{8}\right)^2 \\ &= \left(\frac{\sqrt{2+\sqrt{2}}}{2} + \frac{\sqrt{2-\sqrt{2}}}{2}i\right)^2 \\ &= \frac{\sqrt{2}}{2} + \frac{\sqrt{2}}{2}i \end{aligned}$$

which has order 8 since $(q^2)^8 = 1$. Here we have that

$$N(q^2) = q^2\overline{q^2} = \left(\frac{\sqrt{2}}{2} + \frac{\sqrt{2}}{2}i\right)\left(\frac{\sqrt{2}}{2} - \frac{\sqrt{2}}{2}i\right) = \frac{1}{2} + \frac{1}{2} = 1$$

as required and get the trace

$$Tr(q^2) = 2\left(\frac{\sqrt{2}}{2}\right) = \sqrt{2}$$

as required. However, we still need to show that $-\sqrt{2}$ can also be the trace of order 8 elements of S^3. So now we try and see if $-q^2$ is of order 8. We have

$$-q^2 = -\frac{\sqrt{2}}{2} - \frac{\sqrt{2}}{2}i$$

which has order 8 since $(-q^2)^8 = 1$. Here we have that

$$N(-q^2) = (-q^2)(\overline{-q^2}) = \left(-\frac{\sqrt{2}}{2} - \frac{\sqrt{2}}{2}i\right)\left(-\frac{\sqrt{2}}{2} + \frac{\sqrt{2}}{2}i\right) = \frac{1}{2} + \frac{1}{2} = 1$$

as required and get the trace

$$Tr(-q^2) = 2\left(-\frac{\sqrt{2}}{2}\right) = -\sqrt{2}$$

as required. So we have shown that order 8 elements of S^3 have trace $\pm\sqrt{2}$.

Order 10: Consider a quaternion representing a 36° rotation ($\theta = \frac{\pi}{5}$) around the axis $u = i$. This rotation has order 10 and can be represented by $B(q)$ where

$$\begin{aligned} q &= \cos\frac{1}{2}\theta + u\sin\frac{1}{2}\theta \\ &= \cos\frac{\pi}{10} + i\sin\frac{\pi}{10} = \frac{1}{4}\sqrt{10+2\sqrt{5}} + \frac{1}{4}(\sqrt{5}-1)i. \end{aligned}$$

However, here we have $q^{10} = -1$ which means that q has order 20. So we try and solve this problem by checking if $-q$ has order 10. We have

$$-q = -\cos\frac{\pi}{10} - i\sin\frac{\pi}{10} = -\frac{1}{4}\sqrt{10+2\sqrt{5}} - \frac{1}{4}(\sqrt{5}-1)i$$

but we still have $(-q)^{10} = -1$. Now we check if q^2 is of order 10. Recall that for $B(q)$ of order 5 earlier in this example we had q of order 10. Therefore we can just let q^2 here be equal to that q. Thus we have

$$q^2 = \frac{1+\sqrt{5}}{4} + \left(\sqrt{\frac{5}{8} - \frac{\sqrt{5}}{8}}\right)i$$

which gives us $(q^2)^{10} = 1$ meaning that it has order 10. Then we get

$$\begin{aligned} N(q^2) &= q^2\overline{q^2} \\ &= \left(\frac{1+\sqrt{5}}{4} + \left(\sqrt{\frac{5}{8} - \frac{\sqrt{5}}{8}}\right)i\right)\left(\frac{1+\sqrt{5}}{4} - \left(\sqrt{\frac{5}{8} - \frac{\sqrt{5}}{8}}\right)i\right) \\ &= \frac{3+\sqrt{5}}{8} + \frac{5-\sqrt{5}}{8} \\ &= 1 \end{aligned}$$

as required. Thus we get the following trace:

$$Tr(q^2) = 2\left(\frac{1+\sqrt{5}}{4}\right) = \frac{1}{2}(1+\sqrt{5}) = \tau$$

as required. However, we still need to show that $-\tau^{-1} = \frac{1-\sqrt{5}}{2}$ can also be the trace of order 10 elements of S^3. So now we try and see if $-q^2$ is of order 10. We get.

$$-q^2 = \frac{1-\sqrt{5}}{4} - \left(\sqrt{\frac{5}{8} + \frac{\sqrt{5}}{8}}\right) i$$

which has order 10 since $(-q^2)^{10} = 1$. Here we have that

$$\begin{aligned}
N(-q^2) &= (-q^2)(\overline{-q^2}) \\
&= \left(\frac{1-\sqrt{5}}{4} - \left(\sqrt{\frac{5}{8} + \frac{\sqrt{5}}{8}}\right) i\right)\left(\frac{1-\sqrt{5}}{4} + \left(\sqrt{\frac{5}{8} + \frac{\sqrt{5}}{8}}\right) i\right) \\
&= \left(\frac{1-\sqrt{5}}{4}\right)^2 - \left(\frac{5}{8} + \frac{\sqrt{5}}{8}\right) i^2 \\
&= \frac{3-\sqrt{5}}{8} + \frac{5}{8} + \frac{\sqrt{5}}{8} \\
&= 1
\end{aligned}$$

as required. Thus we get the following trace:

$$Tr(-q^2) = 2\left(\frac{1-\sqrt{5}}{4}\right) = \frac{1-\sqrt{5}}{2} = -\tau^{-1}$$

as required. So we have shown that order 10 elements of S^3 have trace τ or $-\tau^{-1}$ where $\tau = \frac{1}{2}(1+\sqrt{5})$.

In Example 4.2.1 we see that $B(q)$ represents a rotation of angle θ about axis u with $q = \cos\frac{1}{2}\theta + u \sin\frac{1}{2}\theta$. However, we see that if $B(q)$ has order n, then q has order $2n$. If we let $u = i$, notice that

$$\begin{aligned}
q &= \cos\frac{1}{2}\theta + i\sin\frac{1}{2}\theta \\
&= \cos\frac{2\pi}{2n} + i\sin\frac{2\pi}{2n} \qquad \left(\text{Since } \theta = \frac{2\pi}{n} \text{ when } B(q) \text{ has order } n\right) \\
&= \exp\left(\frac{2\pi i}{2n}\right) \\
&= \zeta_{2n}.
\end{aligned}$$

Since $q = \zeta_{2n}$, we have that $q \in \mathcal{D}_{2n}$. Therefore $q^{2n} = 1$ by the definition of the binary dihedral group which is the reason that $B(q)$ being a rotation of order n implies that q has order $2n$. In Figures 4.2-4.4 we see that ζ_n represents the n^{th} roots of unity. So for example, if the order of $B(q)$ is $n = 4$, then $q = \zeta_{2n} = \zeta_8$ meaning that q has order 8. Hence why in Example 4.2.1 we calculated the trace using $q^2 = (\zeta_8)^2 = \zeta_4$ since ζ_4 has order 4.

However, when calculating the trace of q with order 5, it was not enough just to calculate the trace for $\zeta_5 = (\zeta_{10})^2$ since the trace table tells us that there are two possible trace values for elements of order 5 ($-\tau, \tau^{-1}$ where $\tau = \frac{1}{2}(1+\sqrt{5})$). For $B(q)$ of order 5 we have $q = \zeta_{10}$ of order 10. Instead of squaring q, it is also possible to negate q in this case to get an element of order 5. This is because $-\zeta_{10} = (\zeta_5)^3$ as we see in Figure 4.4. Since we have a negative q it means that the trace will also be negative, which is why there is a second value for the trace in this case.

For Example 4.2.1, since there were multiple different ways of arriving at a value for q of the correct order, it meant that we needed to check all the possibilities. In other words, we had to check the order of q, $-q$, q^2, and even $-q^2$ until we got a value of the correct order and calculated all the traces from the trace table.

By using the trace table, we can see that an element $\omega := \frac{1}{2}(-1+i+j+k)$ has order 3 since $Tr(\omega) = 2(\frac{1}{2}(-1)) = -1$. It follows that ω normalises $\mathcal{Q}$ as we show by direct calculation in the following example.

Example 4.2.2. Remember that $\mathcal{Q} = \{\pm 1, \pm i, \pm j, \pm k\}$, and we need to check that $\omega \mathcal{Q} \omega^{-1} = \mathcal{Q}$ to see that ω normalises $\mathcal{Q}$. To do so, we need to check that $\omega q \omega^{-1} \in \mathcal{Q}$ for all $q \in \mathcal{Q}$. Note that $\omega^{-1} = \omega^2$ in this case since ω has order 3. We first calculate $\omega^2 = \frac{1}{2}(-1-i-j-k) = \omega^{-1}$ and then calculate $\omega q \omega^{-1}$ for elements $q \in \mathcal{Q}$ as follows.

$\underline{q = 1, -1}$: For $q = 1, -1$ we have

$$\begin{aligned} \omega q \omega^{-1} &= \omega \omega^{-1} q && \text{(Since real numbers commute with } \mathbb{H}\text{)} \\ &= q \in \mathcal{Q} \end{aligned}$$

as required.

$\underline{q = i, -i}$: We have

$$\begin{aligned}
\omega(i)\omega^{-1} &= \frac{1}{2}(-1+i+j+k)(i)\frac{1}{2}(-1-i-j-k) \\
&= \frac{1}{4}(-1+i+j+k)(-i-i^2-ij-ik) \\
&= \frac{1}{4}(-1+i+j+k)(1-i+j-k) \\
&= \frac{1}{4}(-1+i-j+k+i-i^2+ij-ik+j-ji+j^2-jk+k-ki+kj-k^2) \\
&= \frac{1}{4}(k+k+k+k) = k \in \mathcal{Q},
\end{aligned}$$

which we get due to cancellation. Clearly we also have $\omega(-i)\omega^{-1} = \omega(-1)(i)\omega^{-1} = -\omega(i)\omega^{-1} = -k \in \mathcal{Q}$, as required.

$\underline{q = j, -j}$: Next we have

$$\begin{aligned}
\omega(j)\omega^{-1} &= \frac{1}{2}(-1+i+j+k)(j)\frac{1}{2}(-1-i-j-k) \\
&= \frac{1}{4}(-1+i+j+k)(-j-ji-j^2-jk) \\
&= \frac{1}{4}(-1+i+j+k)(1-i-j+k) \\
&= \frac{1}{4}(-1+i+j-k+i-i^2-ij+ik+j-ji-j^2+jk+k-ki-kj+k^2) \\
&= \frac{1}{4}(i+i+i+i) = i \in \mathcal{Q},
\end{aligned}$$

which we get due to cancellation. Clearly we also have $\omega(-j)\omega^{-1} = \omega(-1)(j)\omega^{-1} = -\omega(j)\omega^{-1} = -i \in \mathcal{Q}$, as required.

$\underline{q = k, -k}$: Finally, for $q = k$ we have

$$\begin{aligned}
\omega(k)\omega^{-1} &= \omega(ij)\omega^{-1} \\
&= \omega(i)\omega^{-1}\omega(j)\omega^{-1} && \text{(Since } \omega^{-1}\omega = 1) \\
&= ki = j \in \mathcal{Q}
\end{aligned}$$

as required. Clearly we also have $\omega(-k)\omega^{-1} = \omega(-1)(k)\omega^{-1} = -\omega(k)\omega^{-1} = -j \in \mathcal{Q}$.

So we have shown that $\omega\mathcal{Q}\omega^{-1} = \mathcal{Q}$, meaning that ω does normalise $\mathcal{Q}$.

Thus we get the following definition.

Definition 4.2.3 (Binary Tetrahedral Group [1])**.** The *binary tetrahedral group* is given by $\mathcal{T} := \mathcal{Q}\langle\omega\rangle = \{q, q\omega, q\omega^2 \mid q \in \mathcal{Q}\}$ and is of order 24. It can be generated by i and ω.

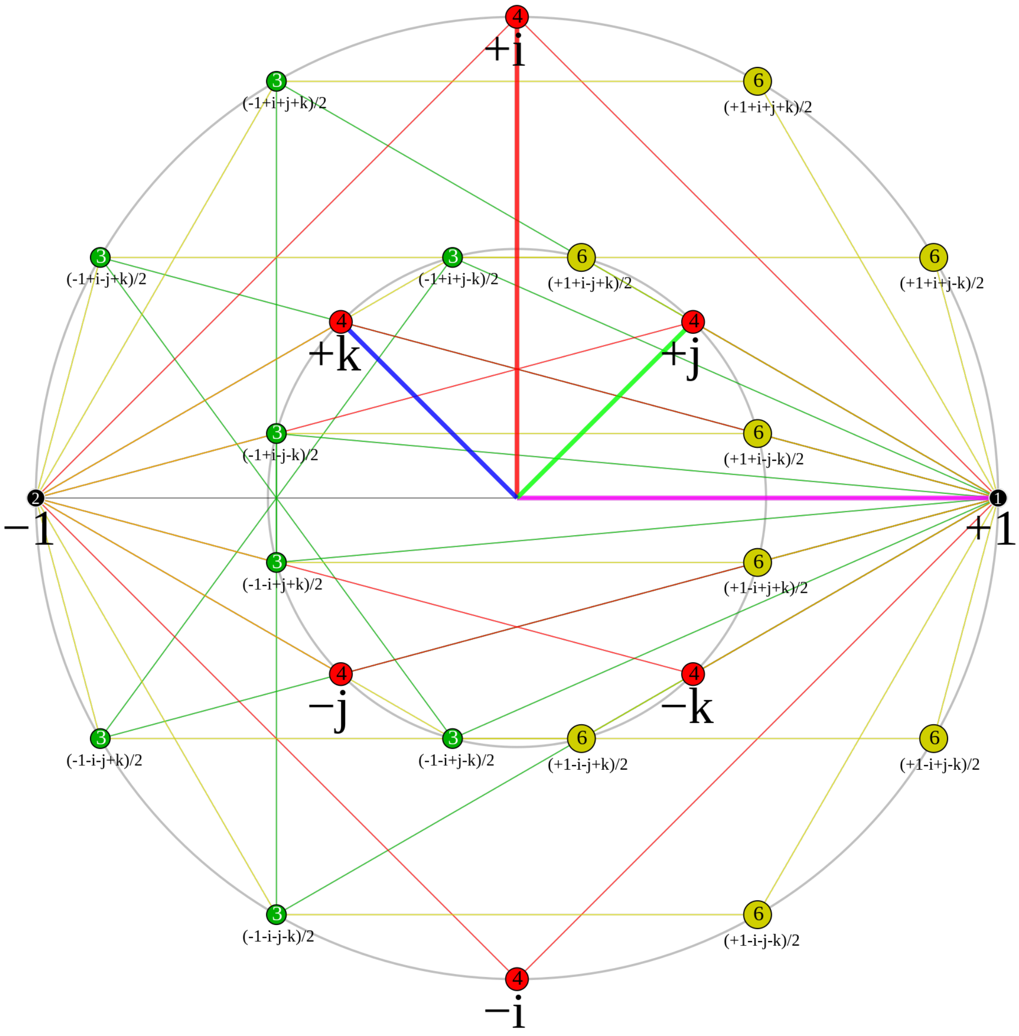

Figure 4.5: Binary Tetrahedral Group Diagram [10].

We also have that $\mathcal{T} \backslash \mathcal{Q}$ consists of the 16 elements of the form $\frac{1}{2}(\pm 1 \pm i \pm j \pm k)$. Therefore, these 16 elements along with the elements in $\mathcal{Q}$ make up the quaternion elements of $\mathcal{T}$, and these elements have the following orders.

order	1	2	3	4	6
element	1	-1	$\frac{1}{2}(-1 \pm i \pm j \pm k)$	$\pm i, \pm j, \pm k$	$\frac{1}{2}(1 \pm i \pm j \pm k)$

All these elements have norm 1 which means that the binary tetrahedral group is a subgroup of the unit quaternions S^3. Thus, the binary tetrahedral group is a finite subgroup of $\mathbb{H}\backslash\{0\}$. Figure 4.5 shows us a diagram of the elements in $\mathcal{T}$ and visualises the results from the table above, giving the order of each element in the coloured dots. The diagram is a 2D projection of a sphere, so it also shows that every element in $\mathcal{T}$ lies on the unit sphere in 4-dimensional space (i.e. in S^3).

By using the trace table, we can also see that the element $\gamma := \frac{1}{\sqrt{2}}(1+i)$ has order 8 since we have

$$Tr(\gamma) = 2\left(\frac{1}{\sqrt{2}}(1+i)\right) = 2\left(\frac{1}{\sqrt{2}}(1)\right) = \frac{2}{\sqrt{2}} = \sqrt{2}.$$

Now we will show by direct calculation that γ normalises the binary tetrahedral group $\mathcal{T}$.

Example 4.2.4. In this example, we are checking that γ normalises $\mathcal{T}$. Since $\mathcal{T} = \omega\mathcal{Q}$, we will first check that γ normalises $\mathcal{Q}$. We will do the same as we did when checking that ω normalises $\mathcal{Q}$. Note that $\gamma^{-1} = \gamma^7$ in this case since γ has order 8. We first calculate $\gamma^7 = \gamma^3\gamma^4 = \gamma^3(\gamma^2)^2 = \frac{1}{\sqrt{2}}(1-i) = \gamma^{-1}$ and then calculate $\gamma q\gamma^{-1}$ for elements $q \in \mathcal{Q}$ as follows.

$\underline{q = 1, -1}$: In a similar way as in Example 4.2.2, for $q = 1, -1$ we have

$$\gamma q\gamma^{-1} = \gamma\gamma^{-1}q = q \in \mathcal{Q}$$

as required.

$\underline{q = i, -i}$: We have

$$\begin{aligned}
\gamma(i)\gamma^{-1} &= \frac{1}{\sqrt{2}}(1+i)(i)\frac{1}{\sqrt{2}}(1-i) \\
&= \frac{1}{2}(1+i)i(1-i) \\
&= \frac{1}{2}(1+i)(i+1) \\
&= \frac{1}{2}(i+1+i^2+i) = i \in \mathcal{Q},
\end{aligned}$$

as required. Clearly we also have $\gamma(-i)\gamma^{-1} = \gamma(-1)(i)\gamma^{-1} = -\gamma(i)\gamma^{-1} = -i \in \mathcal{Q}$.

$\underline{q = j, -j}$: Next we have

$$\begin{aligned}\gamma(j)\gamma^{-1} &= \frac{1}{\sqrt{2}}(1+i)(j)\frac{1}{\sqrt{2}}(1-i) \\ &= \frac{1}{2}(1+i)j(1-i) \\ &= \frac{1}{2}(1+i)(j+k) \\ &= \frac{1}{2}(j+k+k-j) = k \in \mathcal{Q},\end{aligned}$$

as required. Clearly we also have $\gamma(-j)\gamma^{-1} = \gamma(-1)(j)\gamma^{-1} = -\gamma(j)\gamma^{-1} = -k \in \mathcal{Q}$.

$\underline{q = k, -k}$: Finally, for $q = k$ we have

$$\begin{aligned}\gamma(k)\gamma^{-1} &= \gamma(ij)\gamma^{-1} \\ &= \gamma(i)\gamma^{-1}\gamma(j)\gamma{-1} && \text{(Since } \gamma^{-1}\gamma = 1) \\ &= ik = -j \in \mathcal{Q}\end{aligned}$$

as required. Clearly we also have $\gamma(-k)\gamma^{-1} = \gamma(-1)(k)\gamma^{-1} = -\gamma(k)\gamma^{-1} = j \in \mathcal{Q}$.

So we have shown that $\gamma\mathcal{Q}\gamma^{-1} = \mathcal{Q}$, meaning that γ does normalise $\mathcal{Q}$.
Now we will show that γ normalises the whole of the tetrahedral group $\mathcal{T}$. Firstly, we check that $\gamma\omega\gamma \in \mathcal{T}$. Remember that $\omega = \frac{1}{2}(-1+i+j+k)$. Then we get

$$\begin{aligned}\gamma\omega\gamma^{-1} &= \frac{1}{\sqrt{2}}(1+i)\frac{1}{2}(-1+i+j+k)\frac{1}{\sqrt{2}}(1-i) \\ &= \frac{1}{4}(-2+2k)(1-i) \\ &= \frac{1}{2}(-1+i-j+k) \\ &= (-i)\frac{1}{2}(-1-i-j-k) \\ &= -i\omega^2 \in \mathcal{T}\end{aligned}$$

by definition. Thus, to see that γ normalises every element in $\mathcal{T}$ we check that $\gamma(q\omega^k)\gamma^{-1}$ for $k \in \{0,1,2\}$, since $\mathcal{T} = \{q\omega^k \mid k \in \{0,1,2\}, q \in \mathcal{Q}\}$. We have

$$\gamma(q\omega^k)\gamma^{-1} = (\gamma q\gamma^{-1})(\gamma\omega\gamma^{-1})^k \in \mathcal{Q}\cdot\mathcal{T} = \mathcal{T},$$

as required. Hence γ normalises the binary tetrahedral group, $\mathcal{T}$.

We will now define the group generated by γ.

Definition 4.2.5 (Binary Octahedral Group [1])**.** The *binary octahedral group* is given by $\mathcal{O} := \mathcal{T}\langle\gamma\rangle = \{t, t\gamma \mid t \in \mathcal{T}\}$ and is of order 48. It can be generated by ω and γ.

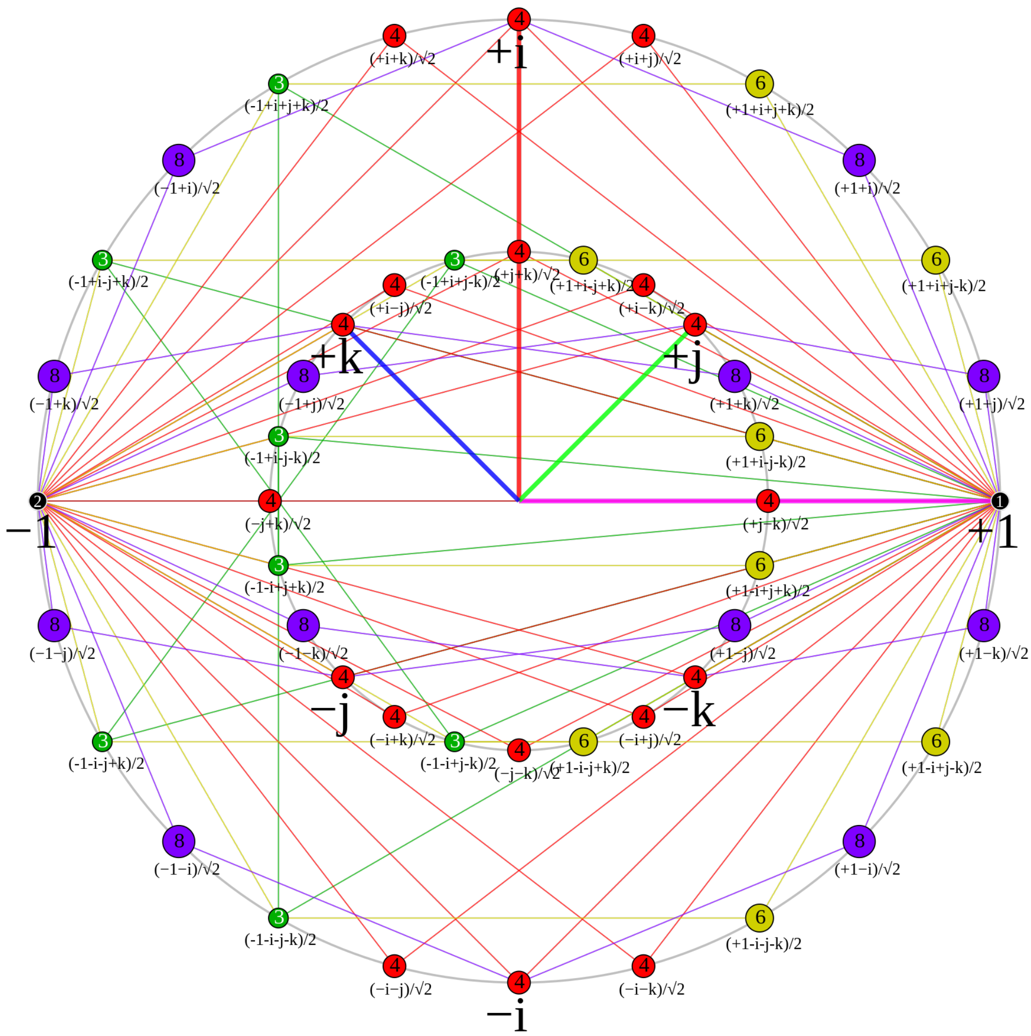

Figure 4.6: Binary Octahedral Group Diagram [11].

We have that $\mathcal{T}\langle\gamma\rangle$ has order 48 because it is given by $\{t, t\gamma \mid t \in \mathcal{T}\}$ and there are 24 elements $t \in \mathcal{T}$. Even though γ is of order 8, we do not have unique elements $t\gamma^k$ for $k \geq 2$ since $\gamma^2 = i \in \mathcal{T}$. We also have that $\mathcal{O}\backslash\mathcal{T}$ consists of 24 elements of the from $\frac{1}{\sqrt{2}}(\pm q \pm r)$, where q and r are distinct elements of $\{1, i, j, k\}$. Of these 24 elements, there are 12 of the form $\frac{1}{\sqrt{2}}(\pm 1 \pm v)$, where $v \in \{i, j, k\}$. By using the trace table, we see that these elements have order 8 since we have

$$Tr\left(\frac{1}{\sqrt{2}}(\pm 1 \pm v)\right) = 2\left(\pm\frac{1}{\sqrt{2}}\right) = \pm\sqrt{2}.$$

The other 12 elements of $\mathcal{O}\backslash\mathcal{T}$ are of the form $\frac{1}{\sqrt{2}}(\pm u \pm v)$, where u and v are distinct elements of $\{i, j, k\}$. By looking at the trace table, we see that these elements have order 4 since

$$Tr\left(\frac{1}{\sqrt{2}}(\pm u \pm v)\right) = 2(0) = 0.$$

Therefore, these 24 elements along with the elements in $\mathcal{T}$ make up the quaternion elements of $\mathcal{O}$, and these elements have the orders from the the table for $\mathcal{T}$ along with the following.

order	4	8
element	$\pm\frac{1}{\sqrt{2}}(\pm u \pm v)$	$\frac{1}{\sqrt{2}}(\pm 1 \pm v)$

All these elements have norm 1 which means that the binary octahedral group is a subgroup of the unit quaternions S^3. Thus, the binary octahedral group is a finite subgroup of $\mathbb{H}\backslash\{0\}$. Figure 4.6 shows us a diagram of the elements in $\mathcal{O}$ and visualises the results from the two tables above, giving the order of each element in the coloured dots. The diagram is a 2D projection of a sphere, so it also shows that every element in $\mathcal{O}$ lies on the unit sphere in 4-dimensional space (i.e in S^3).

By using the trace table, we can also see that the element $\sigma := \frac{1}{2}(\tau^{-1} + i + \tau j)$ has order 5 (where $\tau = \frac{1}{2}(1 + \sqrt{5})$) since

$$\begin{aligned} Tr(\sigma) &= 2\left(\frac{1}{2}\left(\frac{-1+\sqrt{5}}{2} + i + \frac{1+\sqrt{5}}{2}j\right)\right) \\ &= \frac{-1+\sqrt{5}}{2} = \tau^{-1}. \end{aligned}$$

The following results about σ and the binary icosahedral group come straight from Lehrer and Taylor's, "Unitary Reflection Groups" [1], and we will not prove the results stated. The element σ acts on the space V of pure quaternions via the homomorphism $B : S^3 \to SO(\mathbb{R})$ from Proposition 3.2.9. The 12 vectors $\pm\tau i \pm j$, $\pm\tau j \pm k$ and

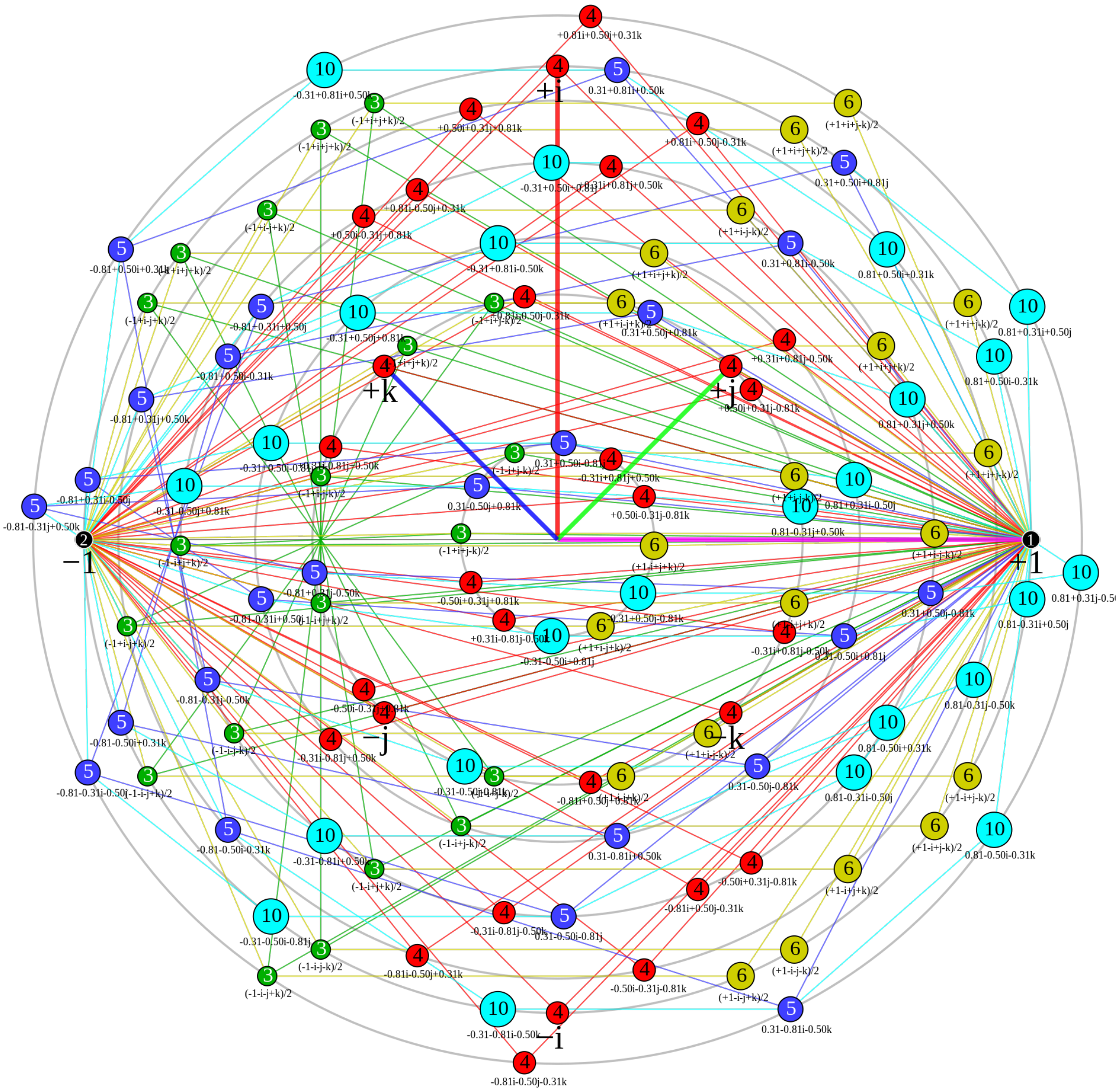

Figure 4.7: Binary Icosahedral Group Diagram [12].

$\pm\tau k \pm i$ form the vertices of a regular icosahedron in V (the regular polyhedron with 12 vertices) and they are permuted among themselves by $B(t)$ and by $B(\sigma)$ where $t \in \mathcal{T}$. Only ± 1 can fix all six lines spanned by these vectors. Thus the group generated by $\mathcal{T}$ and σ is finite.

Definition 4.2.6 (Binary Icosahedral Group [1])**.** The group $\mathcal{I}$ spanned by the vectors $\pm\tau i \pm j$, $\pm\tau j \pm k$ and $\pm\tau k \pm i$ is the *binary icosahedral group* and is of order 120. It can be generated by σ and i.

Figure 4.7 shows us a diagram of the elements in $\mathcal{I}$ and shows us that every element in $\mathcal{I}$ has an order of $1, 2, 3, 4, 5, 6, 8$, or 10. In example 4.2.1, we verified the traces of elements in S^3 of these orders by using the representation of $B(q)$ as a rotation where $q \in S^3$. Therefore, since $B(q)$ maps elements of these orders, it means that $B(q)$ maps every element in the binary icosahedral group. Therefore, the binary icosahedral group, $\mathcal{I}$, is a finite subgroup of the unit quaternions, S^3. In the same way as Figures 4.5 and 4.6, the diagram also shows that every element in $\mathcal{I}$ lies on the unit sphere in 4-dimensional space (i.e. in S^3).

Now that we have seen that $\mathcal{C}_n$, $\mathcal{D}_{2n}$, $\mathcal{T}$, $\mathcal{O}$, and $\mathcal{I}$ are all finite subgroups of $\mathbb{H}\backslash\{0\}$, we have the final theorems of the project. These results come from Lehrer and Taylor's book, "Unitary Reflection Groups" [1] and are as follows.

Theorem 4.2.7. *Every finite subgroup of $\mathbb{H}\backslash\{0\}$ is conjugate in S^3 to one of the following groups:*

(i) the cyclic group $\mathcal{C}_n$,

(ii) the binary dihedral group $\mathcal{D}_{2n}$,

(iii) the binary tetrahedral group $\mathcal{T}$ of order 24,

(iv) the binary octahedral group $\mathcal{O}$ of order 48,

(v) the binary icosahedral group $\mathcal{I}$ of order 120.

We will not prove that the finite subgroups in Theorem 4.2.7 are conjugate in S^3 to every finite subgroup of $\mathbb{H}\backslash\{0\}$. This is a long proof and is given by Lehrer and Taylor [1]. This is an interesting fact about the quaternions and by earlier results from the project, we can see that this theorem can be rewritten to show the finite subgroups of the special orthogonal group $SO_3(\mathbb{R})$ and the special unitary group $SU_2(\mathbb{C})$.

By the homomorphism of Proposition 3.2.10 we can rewrite Theorem 4.2.7 in terms of subgroups of $SO_3(\mathbb{R})$.

Theorem 4.2.8. *Every finite subgroup of $SO_3(\mathbb{R})$ is conjugate in $SO_3(\mathbb{R})$ to one of the following groups:*

(i) the cyclic group generated by

$$\begin{bmatrix} 1 & 0 & 0 \\ 0 & cos(\frac{4\pi}{n}) & -sin(\frac{4\pi}{n}) \\ 0 & sin(\frac{4\pi}{n}) & cos(\frac{4\pi}{n}) \end{bmatrix},$$

(ii) the dihedral group generated by

$$\begin{bmatrix} 1 & 0 & 0 \\ 0 & cos(\frac{4\pi}{n}) & -sin(\frac{4\pi}{n}) \\ 0 & sin(\frac{4\pi}{n}) & cos(\frac{4\pi}{n}) \end{bmatrix} \textit{ and } \begin{bmatrix} -1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & -1 \end{bmatrix},$$

(iii) the tetrahedral group $\mathcal{T}/\langle -1 \rangle \simeq A_4$ generated by

$$\begin{bmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 0 & 0 \end{bmatrix} \textit{ and } \begin{bmatrix} 1 & 0 & 0 \\ 0 & -1 & 0 \\ 0 & 0 & -1 \end{bmatrix},$$

(iv) the octahedral group $\mathcal{O}/\langle -1 \rangle \simeq S_4$ generated by

$$\begin{bmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 0 & 0 \end{bmatrix} \textit{ and } \begin{bmatrix} 1 & 0 & 0 \\ 0 & 0 & -1 \\ 0 & 1 & 0 \end{bmatrix},$$

(v) the icosahedral group $\mathcal{I}/\langle -1 \rangle \simeq A_5$ generated by

$$\frac{1}{2}\begin{bmatrix} 1 & \tau & \tau^{-1} \\ \tau & -\tau^{-1} & -1 \\ -\tau^{-1} & 1 & -\tau \end{bmatrix} \textit{ and } \begin{bmatrix} 1 & 0 & 0 \\ 0 & -1 & 0 \\ 0 & 0 & -1 \end{bmatrix}, \textit{ where } \tau = \frac{1}{2}(1+\sqrt{5}).$$

Similarly, by the isomorphism of Proposition 3.3.6 we can also rewrite Theorem 4.2.7 in terms of subgroups of $SU_2(\mathbb{C})$.

Theorem 4.2.9. *Every finite subgroup of $SU_2(\mathbb{C})$ is conjugate in $SU_2(\mathbb{C})$ to one of the following groups:*

(i) the cyclic group $\mathcal{C}_n$ of order n generated by

$$\begin{bmatrix} e^{\frac{2\pi i}{n}} & 0 \\ 0 & e^{-\frac{2\pi i}{n}} \end{bmatrix},$$

(ii) the binary dihedral group $\mathcal{D}_{2n}$ of order $4n$ generated by

$$\begin{bmatrix} e^{\frac{\pi i}{n}} & 0 \\ 0 & e^{-\frac{\pi i}{n}} \end{bmatrix} \quad \textit{and} \quad \begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix},$$

(iii) the binary tetrahedral group $\mathcal{T}$ of order 24 generated by

$$\frac{1}{2}\begin{bmatrix} -1-i & 1-i \\ -1-i & -1+i \end{bmatrix} \quad \textit{and} \quad \begin{bmatrix} -i & 0 \\ 0 & i \end{bmatrix},$$

(iv) the binary octahedral group $\mathcal{O}$ of order 48 generated by

$$\frac{1}{2}\begin{bmatrix} -1-i & 1-i \\ -1-i & -1+i \end{bmatrix} \quad \textit{and} \quad \frac{1}{\sqrt{2}}\begin{bmatrix} 1-i & 0 \\ 0 & 1+i \end{bmatrix},$$

(v) the binary icosahedral group $\mathcal{I}$ of order 120 generated by

$$\frac{1}{2}\begin{bmatrix} \tau^{-1}-\tau i & 1 \\ -1 & \tau^{-1}+\tau i \end{bmatrix} \quad \textit{and} \quad \begin{bmatrix} -i & 0 \\ 0 & i \end{bmatrix}, \quad \textit{where } \tau = \frac{1}{2}(1+\sqrt{5}).$$

These results are very useful in group theory as they show that up to conjugacy, there are only five possible finite subgroups of $\mathbb{H}\backslash\{0\}$, $SO_3(\mathbb{R})$, and $SU_2(\mathbb{C})$. I may not have proved these theorems, but what I have learned throughout the whole project leading up to these results has built up a good understanding of what the theorems mean. Working on this project as a whole has improved my ability to construct proofs and has developed my understanding of algebra and group theory which is my principal gain from completing this project.

To see what can be learned beyond what has been achieved in this project, one can read Lehrer and Taylor's book, "Unitary Reflection Groups" [1]. After they prove Theorem 4.2.7 about the finite subgroups of $\mathbb{H}\backslash\{0\}$, they write about isomorphisms of these finite subgroups. Any group that is isomorphic to a finite subgroup of $\mathbb{H}\backslash\{0\}$ will itself be a finite subgroup of $\mathbb{H}\backslash\{0\}$. Since the book is about unitary reflection groups, they move on to finding ways to determine which elements of the unitary group $U_2(\mathbb{C})$ are reflections and use some of the results that we have seen in this project to do so.

Bibliography

[1] Lehrer, G. and Taylor, D.E. (2009) *Unitary reflection groups*. Cambridge, UK: Cambridge University Press.

[2] Pierce, R.S. (1982) *Associative algebras*. New York: Springer.

[3] Dummit, D.S. and Foote, R.M. (2004) *Abstract algebra*. Danvers: John Wiley & Sons.

[4] Towers, M. (2022) 4.16 the rank-nullity theorem, 4.16 The rank-nullity theorem - Chapter 4 Linear algebra - MATH0005 Algebra 1 - Chapter 4 Linear algebra - MATH0005 Algebra 1. Available at: https://www.ucl.ac.uk/ ucahmto/0005_2021/Ch4.S16.html (Accessed: 05 May 2024).

[5] Coxeter, H.S.M. and Greitzer, S.L. (1997) *Geometry revisited*. New York: Mathematical Assoc. of America.

[6] Axler, S.J. (2024) *Linear algebra done right*. Cham: Springer.

[7] Alcock-Zeilinger, J. (2018) The Special Unitary Group, Birdtracks, and Applications in QCD. Available at: https://www.math.uni-tuebingen.de/de/forschung/maphy/lehre/ss-2018/sun/dateien/birdtracks-sun-qcd-lecturenotes.pdf (Accessed: 05 May 2024).

[8] Dihedral group/examples (no date) ProofWiki. Available at: https://proofwiki.org/wiki/Dihedral_Group/Examples (Accessed: 05 May 2024).

[9] MATLAB, 2023. version 23.2.0 (R2023b), Natick, Massachusetts: The MathWorks Inc.

[10] Tomruen (2022) Binary Tetrahedral Group, Wikipedia. Available at: https://en.wikipedia.org/wiki/Binary_tetrahedral_group#/media/File:Binary_tetrahedral_group_elements_12-fold.svg (Accessed: 05 May 2024).

[11] Tomruen (2021) Binary Octahedral Group, Wikipedia. Available at: https://en.wikipedia.org/wiki/Binary_octahedral_group#/media/File:Binary_octahedral_groupelements_12-fold.svg (Accessed: 05 May 2024).

[12] Tomruen (2024) Binary Icosahedral Group, Wikipedia. Available at: https://en.wikipedia.org/wiki/Binary_icosahedral_group#/media/File:Binary_icosahedral_group_elements_12-fold.svg (Accessed: 05 May 2024).